From Skin to Screen: Bodily Integrity in the Digital Age

Júlia Keserű, November 2024

Contents

From Skin to Screen: Bodily Integrity in the Digital Age

Written by Júlia Keserű

Senior Tech Policy Fellow, Mozilla Foundation
Budapest, November 2024

This report and its associated products are the outcome of a 24-month Mozilla Fellowship.

Credits
Supported by moz://a

Thanks to the following individuals for their feedback on the research: Becca Ricks, Claire Jenifer Pershan, Lucy Purdon, Reem Suleiman, Sara Baker, and Stefan Baack.

Design and illustrations by Surasti Puri and Tamás Szémann.

Edits by Michael Plessis.

Suggested Citation
Keserű, J. (2024). From Skin to Screen: Bodily Integrity in the Digital Age.

Executive summary

This research paper examines the evolution of structured data collection related to the human body and mind, examining industry trends, promised benefits, associated harms, existing legal protections, and public attitudes toward body-focused data practices.

As the adoption of new technologies like electronic health records, mobile health applications, and biometric systems accelerates, the technology industry is increasingly celebrating the potential benefits of body-focused data collection. However, this rapid advancement raises serious questions, especially as emerging threats highlight the inadequacy of current legal protections and the public's distrust in these systems.

Our research paper aims to provide valuable insights into the complex landscape of body-focused data collection and underscore the need for legal and societal reform. **We identify critical insights into the challenges and opportunities presented by body-focused data practices in today's digital landscape, and propose a new framework centered around the concept of "databody integrity."** This approach advocates for recognizing individuals' rights to control and protect their unique physiological and psychological data, ensuring that data handling aligns with broader human-rights principles like autonomy and dignity. Our insights include several key findings that emphasize the urgent need for reform. These include:

◇ **The market for body-centric data has experienced significant growth in the past decade, with projections indicating substantial future increases.** Electronic health record systems (EHR) are projected to reach around USD 45 billion by 2032, with the mobile health sector expected to grow to between USD 250 billion and USD 350 billion. Additionally, the biometric industry is forecasted to surpass USD 200 billion by 2032. Combined, these figures indicate that the market for body-centric data will exceed USD 500-600 billion by the beginning of the next decade. This represents a significant portion of the broader technology industry and does not even encompass all potential avenues of bodily data collection, such as location tracking, extended reality applications, or CCTV cameras. For context, the global pharmaceutical industry was valued at approximately USD 1.5 trillion in 2022, which highlights the substantial economic impact that body-centric data collection may have in the future.

◇ **The growth of body-focused data collection poses significant risks to individuals and society as a whole, including cybersecurity breaches, data misuse, consent violations, discrimination against vulnerable populations, biometric persecution, and widespread surveillance.** Bodily data has become a prime target for cyber extortion, where hackers access sensitive patient information and demand ransom. There has been a dramatic rise in cybersecurity incidents within public healthcare systems and the mobile health industry, which canparalyze entire nations and endanger many individuals. Consent violations are also increasing, asmental health apps, reproductive health apps, biometric firms, and genetic testing companies

non-consensually share user data with researchers, pharmaceutical companies, and other third parties. Data-driven discrimination is becoming more common due to the misuse of sensitive bodily data, such as leaked health information leading to higher insurance premiums, online gambling platforms targeting at-risk individuals based on identifiable traits, hiring firms excluding people with disabilities using faulty emotion recognition tools, and AI diagnostic models showing lower accuracy for darker-skinned patients. The uncontrolled collection of bodily, especially biometric, data exacerbates these issues, making individuals vulnerable to harmful profiling and intrusive surveillance, particularly in sensitive contexts.

◇ **AI tools significantly exacerbate the challenges of body-focused data collection by amplifying existing harms and introducing new risks.** While AI promises benefits such as improved automation and diagnostic accuracy in health records, personalized recommendations in mobile health, and better analysis of user patterns in biometrics, these advantages depend heavily on the quality of underlying algorithms and training datasets—often leading to biased and discriminatory outcomes. Misinterpretations of bodily data can result in misguided health decisions, particularly concerning mobile health solutions that lack direct medical oversight. Additionally, the pervasive biases of AI models have been shown to contribute to public distrust, especially among marginalized communities, with high misidentification rates for darker-skinned individuals leading to wrongful arrests. Furthermore, the data-intensive nature of AI violates existing privacy frameworks focused on data minimization, increasing the risks of re-identification even from anonymized sources.

◇ **The rise of body-focused data collection has intensified scrutiny of the data broker industry, which specializes in purchasing, selling, and trading personal data to create detailed consumer profiles.** Recent reports reveal alarming practices, showing that data brokers sell information related to mental health diagnoses while retaining personal identifiers such as names and addresses of individuals seeking support. These brokers use various techniques—from scraping public records to employing software development kits (SDKs) in mobile apps—that enable extensive data collection without user consent, effectively transforming apps into tools for rampant data harvesting. As brokers shift their focus from raw data to aggregated insights, they expose sensitive health information through location data while companies often retain personal information despite promises of deletion. In the EU, data brokers are regulated under laws requiring explicit user consent, yet many exploit previously granted permissions; conversely, the U.S. lacks comprehensive federal standards, creating a regulatory gap that permits brokers to operate with minimal oversight, frequently sharing sensitive information with law enforcement. With the projected growth of the data broker industry expected to reach between $400 billion and $600 billion by the end of the decade, the implications of these practices become even more pressing, particularly as compromised data often makes its way to the dark web.

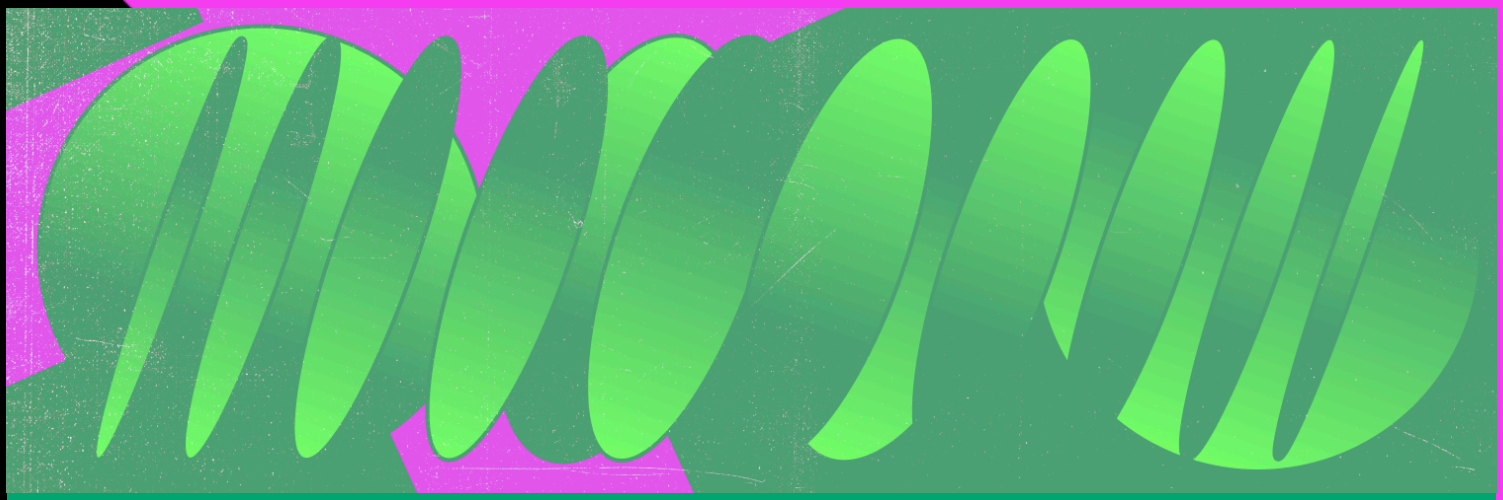
◇ **Existing legal frameworks fall short in addressing the unique challenges posed by body-focused data collection within the context of emerging threats and sophisticated data practices.** There is excessive pressure on data protection laws to safeguard the human body against online harms, but these laws do not offer meaningful remedies. As technology evolves, these frameworks become increasingly outdated, leaving loopholes that can be easily exploited. Ambiguities in the language of these laws create compliance uncertainties, often overwhelming smaller organizations with their complex requirements. Furthermore, in many regions mobile

health solutions operate outside data protection regulations and lack stringent protections for bodily data. The weak enforcement of existing regulations further diminishes their effectiveness. Additionally, the rapid advancement of AI technologies facilitate continuous data processing without clear user awareness, thereby increasing the risk of data misuse. Moreover, current laws often inadequately address the unique vulnerabilities associated with biometric data, heightening concerns about privacy breaches and potential misuse in the public and private sector alike.

◇ **There is a noticeable gap between technological advancements and public expectations for more responsible data handling.** Survey data suggest that while individuals are open to sharing health data for personal benefits—especially for scientific research—concerns about privacy, security, and misuse are prevalent, particularly regarding broader data sharing for profit or without transparency. Acceptance for data sharing for health benefits is accompanied by significant unease about unauthorized access, with many respondents worried about EHR access beyond treating doctors and expressing specifically strong concerns about biometric data sharing. While many felt they could stop using mobile health apps, fewer had the same confidence regarding EHRs and biometric systems, indicating a lack of clarity and control that fuels anxiety around these systems. This disconnect between the optimistic narratives of the technology industry and public sentiment—marked by feelings of anger, fear, and betrayal regarding non-consensual data sharing—highlights an urgent need for clearer regulations and stronger protections for bodily data.

◇ **The examined instances of bodily data harms infringe on fundamental human rights such as autonomy and dignity.** Current legal interpretations often overlook this intersection, necessitating a shift from data protection-centric approaches to a broader rights-focused framework that acknowledges the complex interplay between emerging digital technologies and human rights. In this paper, we advocate for applying existing human rights frameworks, specifically the right to bodily integrity, to address emerging data challenges by introducing the concept of "databody integrity." We propose a new regulatory focus that aligns more closely with autonomy, integrity, and dignity. We also call for strategic litigation to reinforce bodily integrity and push for the implementation of new laws and policies addressing digital threats. To guide these efforts, we also propose a taxonomy that clarifies the relationship between data governance and bodily integrity, categorizing breaches into four critical areas: non-consensual scientific experimentation; non-consensual financial gains; non-consensual bodily modifications; and violations of psychological integrity.

◇ **In response to the pressing challenges posed by body-focused data collection, our paper provides concrete recommendations to enhance the protection of online users.** Policymakers are urged to integrate databody integrity into privacy laws by broadening definitions of sensitive data to include derived and inferred types, reinforcing meaningful consent mechanisms to empower users over their personal information, and adapting regulations to keep pace with technological changes. Activists can advocate for databody integrity through strategic litigation, public awareness campaigns, and the establishment of watchdog groups to ensure corporate accountability. The technology industry must prioritize responsible data management, invest in privacy-enhancing tools, and create transparent and user-centric consent mechanisms to build consumer trust. Individual users should evaluate the implications of sharing their bodily and mental data, utilize resources to assess data practices of devices and applications, maintain strong cybersecurity routines, and manage data permissions effectively to protect their privacy.



Introduction

Context

There has been an exponential growth in the collection of structured data about the human body and mind over the past decade. **The potential benefits of body-focused data collection are diverse, ranging from improved efficiencies in healthcare** (Basil et al, 2022), through cost savings (Tsai et al, 2020), to improved health consciousness (Ahmadian et al, 2015). Biometric data collection promises improved security and better identity verification in various sectors (De Keyser et al, 2021) through increasingly sophisticated and Artificial Intelligence (AI)-driven technologies. However, **as the industry continues to expand, so too do the associated harms.** Workplace and healthcare discrimination (Radhakrishnan, 2021), online harassment (Heller, 2021), cyber extortion (Niki et al, 2022, Javaid et al, 2023), harmful targeting practices (Gak et al, 2022), and biometric persecution (Goldstein and Alonso-Bejarano, 2017, Kingston, 2018, Madianou, 2019, Jacobsen, 2022) are just some of the many negative impacts of body-oriented data collection on consumer and societal health.

Despite the gravity of the issue, current legal protections do not offer meaningful remedies for users adversely affected by body-focused data collection. In the digital realm, there is an excessive focus on data protection regimes as the primary means of safeguarding the human body against online harm. **However, data protection frameworks often cannot address the emerging threats of bodily data collection, especially with recent advancements in data processing and the spread of AI tools** (Renieris, 2023, Blanke, 2020, Van de Waerdt, 2020, Vardanyan et al, 2022, Rupp and Grafenstein, 2024). Current legal definitions do not cover emerging data types like synthetic data (Finck and Pallas, 2020, Van der Slot et al, 2022), while existing definitions of sensitive information are becoming increasingly obsolete given that sophisticated inferences can be made from combining even the most innocent data points (Blanke, 2020). Furthermore, as we outline below, much of the harm caused by these systems goes beyond data protection considerations and violates our fundamental human rights.

Research objectives

Within this context, our research aims to make three important contributions to the emerging field of "body-focused" technologies. First, **we systematically map the key avenues of such data collection by examining industry trends, including how the market is shaped by the rise of AI tools, documenting how prevailing industry practices have jeopardized user safety in the past and analyzing the corresponding legal protections.** In Chapter 1, our analysis centers around the various methods of body-focused data collection, with a special emphasis on electronic health records, mobile health applications, and biometric data, and the harms associated with these practices. In this chapter we will explore and showcase how the rapid evolution of these markets has outpaced governing the collection and use of bodily data. Such public concerns, as we will argue, should serve as a catalyst for re-evaluating and redefining the legal interpretations and protections currently governing body-focused data practices.

Third, we will **investigate the potential role the *right to bodily integrity* could play in protecting users online**, and how established human rights frameworks can be better utilized to address emerging digital threats. Chapter 3 emphasizes the importance of recognizing body-focused data collection as being fundamentally intertwined with individual rights and dignity rather than viewing it solely as a technological or data protection issue. This perspective is crucial, as it acknowledges the complexities and nuances that arise from the interaction between advanced data collection technologies and human experience. By framing these technologies within the context of personal autonomy and bodily integrity, Chapter 3 enhances the arguments made previously about the risks embedded in current data collection practices, and the pressing need for a shift from merely enforcing data protection to advocating for a more robust understanding of human rights in the digital landscape.

Lastly, in Chapter 4 we **provide targeted recommendations for policymakers, activists, technology industry representatives, and individual users, based on our research findings, offering concrete strategies to enhance privacy protections** and address the identified challenges in managing bodily data in our increasingly data-driven world.

Methodology

For this research we deployed **a mixed-methods approach that combined systematic literature and case law reviews, qualitative interviews, and public surveys** to comprehensively examine the complexities surrounding bodily data collection. For our systematic literature review, we utilized targeted combinations of specific search terms[1]. The selection criteria focused on peer-reviewed articles published between 2017 and 2024 that addressed relevant aspects of bodily data collection, the role of AI, existing legal frameworks, and public perceptions, while excluding irrelevant or non-peer-reviewed works. Throughout the review process, we maintained detailed records of the databases searched (including Google Scholar, ScienceDirect, Springer Link, and ResearchGate), the specific search strings used, and the rationale for the selection of studies. Data extraction involved thematic analysis to identify key trends and patterns across the literature, enabling us to synthesize findings and draw meaningful conclusions.

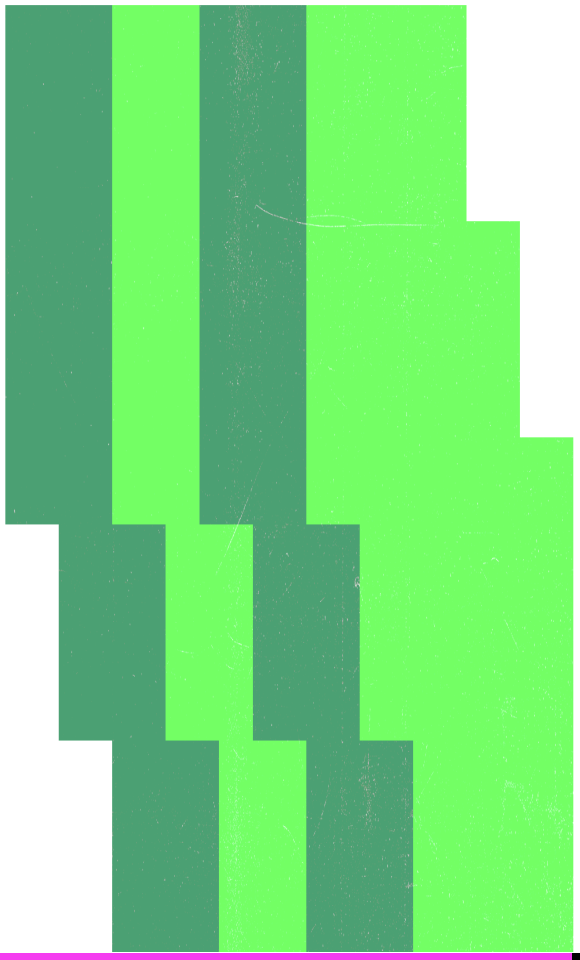
[1] These included "bodily integrity," "digital integrity," "electronic health records," "public health records," "mobile health," "fitness tracking," remote patient monitoring" "biometrics," "behavioral biometrics," "emotion recognition," "facial recognition," "mental health apps," "reproductive health apps", "data privacy," "online privacy," "digital consent," "consent in health data," "consent in biometrics," "data brokers," "data protection," "data protection EU," "data protection US," "AI regulation," and "public attitudes, amongst others.

We also examined pertinent case law surrounding the right to bodily integrity. This involved utilizing Google searches and accessing legal databases such as LexisNexis and the European Court of Human Rights (ECHR) repository to identify relevant judicial rulings. We focused on landmark cases in both the EU and US that have addressed bodily integrity issues.

We also reviewed comprehensive legal analyses found in existing research, including articles from legal journals and reports from organizations like the American Civil Liberties Union (ACLU) and the European Union Agency for Fundamental Rights (FRA). This multi-faceted approach allowed us to weave judicial interpretation and precedent into our understanding of how courts define and protect bodily integrity, particularly in the context of emerging technologies and digital data collection practices.

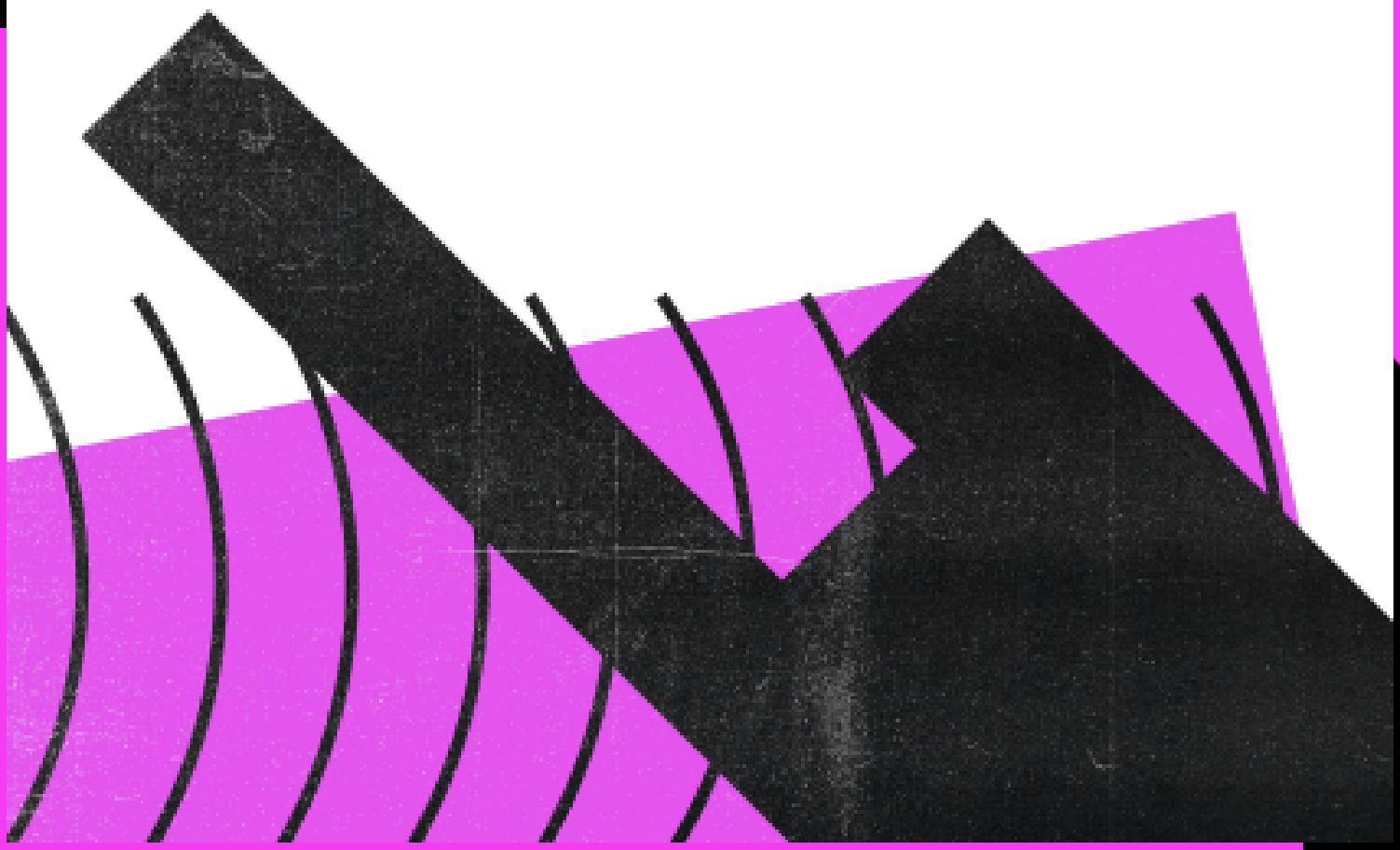
Furthermore, we conducted over 50 interviews with policy experts, academics, health data analysts, software engineers and technology developers to explore the role that the right to bodily integrity could play in online user protection. Interviewees were selected based on their expertise and experience in the relevant fields. We aimed for a diverse range of perspectives, ensuring representation from government, academia, and industry alike. The interview process involved creating a semi-structured guide with open-ended questions aimed at gathering in-depth insights. Key areas of focus included definitions of bodily integrity in digital data collection, challenges and risks associated with bodily data collection, the effectiveness of existing regulatory frameworks, the impact of emerging technologies, especially AI, on bodily integrity, the role of consent in protecting people online, and recommendations for future measures to strengthen protections in the face of increasing data collection.

Additionally, we deployed a series of public surveys to assess general attitudes toward body-focused data collection, in order to complement the qualitative insights gathered from interviews, and to deepen the understanding of public sentiment regarding the topic. These surveys were conducted between June 15 and September 30, 2024 and examined various contextual factors across three key avenues: electronic health records, mobile health apps, and biometric data collection. Utilizing structured questions and Likert scales, the first survey assessed perceptions and concerns regarding electronic health data storage, unauthorized access, control over personal information, and willingness to share data for different purposes. Additionally, we explored respondents' willingness to opt out of data-sharing arrangements and gauged their feelings about sharing bodily data across various contexts, namely for scientific research, law enforcement and financial profit-making.



In contrast, the second survey employed a scenario-based approach by presenting specific, real-world situations related to bodily data sharing in all three avenues. To balance the first survey's quantitative approach, these questions intended to evoke emotional reactions through open-ended questions. Respondents were asked to provide the first three words that came to their mind about scenarios that involved non-consensual bodily data collection in various settings, designed to reflect the taxonomy of the databody integrity framework.

These included cyber attacks in healthcare, sharing fitness data with third-party advertisers, sharing mental health or biometric data for research purposes, access to health records by law enforcement, and the sale of reproductive health and iris scan data to commercial entities without explicit consent. After preprocessing the data, we created sentiment scores and analyzed them to identify key patterns and trends. Additional details about these surveys and their findings can be found in the annex of this paper.



Glossary

Algorithmic bias: The potential for machine learning systems to produce biased outcomes due to unrepresentative training data or flawed algorithms, leading to discriminatory practices.

Artificial intelligence (AI): The simulation of human intelligence processes by machines, particularly computer systems, to enhance diagnostic accuracy and data analysis.

Behavioral biometrics: Techniques analyzing patterns in human behavior, such as typing dynamics or mouse movements, used for continuous authentication processes.

Biometric techniques: Methods of identifying individuals based on unique bodily characteristics, including fingerprint recognition, facial recognition, and DNA testing, often employed in security contexts.

Body-focused data collection: The systematic gathering of data related to an individual's physiological and biological characteristics, impacting privacy and personal rights.

Continuous authentication: An ongoing process of verifying a user's identity based on behavioral and biometric characteristics throughout an interaction session.

Cyber extortion: A form of cybercrime where hackers gain unauthorized access to sensitive data and demand ransoms to avoid public release or to return the data.

Databody integrity: A proposed concept extending the right to bodily integrity into the digital domain, advocating for individuals' control over data reflecting their unique physiological and psychological attributes.

Data brokers: Companies specializing in collecting and trading personal data, creating detailed consumer profiles often without clear user consent or awareness.

Data protection: Mechanisms and regulations designed to safeguard personal information from unauthorized access and ensure privacy.

Electronic health records (EHRs): Digital versions of patients' paper charts, containing comprehensive health data shared among healthcare providers to enhance care quality.

Emotion recognition: Technologies that analyze human emotional states from facial expressions, voice, and physiological signals for various applications, including healthcare and marketing.

Extended reality (XR): Encompasses virtual reality (VR), augmented reality (AR), and mixed reality (MR), technologies that collect and use bodily data to provide immersive experiences.

Facial recognition: A biometric method that identifies individuals by analyzing facial features, used in security and identification processes.

Gait recognition: A biometric technique analyzing the way a person walks to identify and verify their identity.

Image-based abuse: The unauthorized distribution or sharing of intimate images, often compromising privacy and violating personal boundaries.

Informed consent: The process of obtaining explicit permission from individuals before collecting or using their data, ensuring they are fully aware of the implications.

Interoperability: The seamless exchange of health information across different systems and jurisdictions, improving patient care while presenting privacy challenges.

Location tracking: The use of GPS or other technologies to monitor and collect data on an individual's physical whereabouts, often used for marketing or safety purposes.

Mobile health (mHealth) solutions: Technologies like apps and wearable devices that collect real-time data to monitor personal health metrics and support remote patient care.

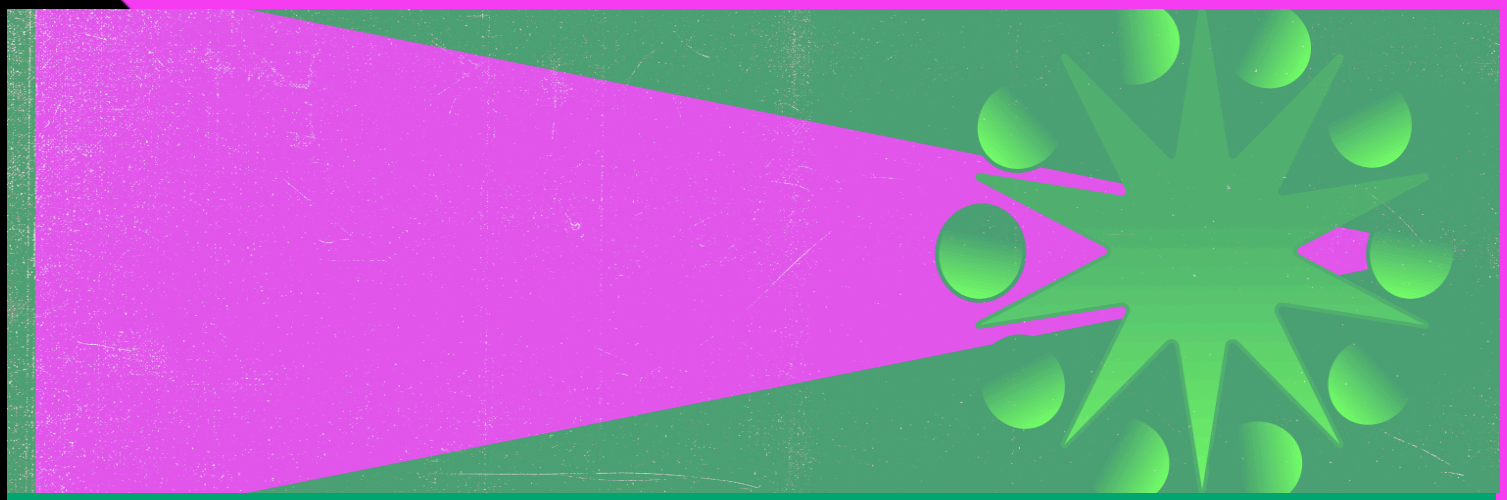
Neurorights: A movement advocating for the protection of individuals' brain data and mental privacy in the face of emerging neurotechnologies.

Odor recognition: A biometric technique using individuals' unique scent profiles for identification purposes.

Predictive analytics: The use of data, statistical algorithms, and machine learning techniques to identify future outcomes based on historical data.

Privacy paradox: The phenomenon where individuals express privacy concerns but continue to share personal data because of perceived benefits.

Strategic litigation: Legal action taken to create broader social change by establishing precedents, often used to advance databody integrity and protect against data abuses.



CHAPTER 1

Body-focused data collection

Body-focused data collection refers to the **systematic gathering of data specifically related to the physiological and biological characteristics of individual users**. This definition emphasizes the intention to capture information that is intricately connected to the human body and its functions, such as health metrics, physical and psychological conditions, and behavioral patterns. In the context of our research, the focus on bodily data is essential for understanding the several ways in which data-driven technologies impact privacy, security, agency, dignity and integrity.This definition serves as the foundation for exploring the many challenges associated with the increasing reliance on body-focused data in the digital age, as outlined throughout the paper.

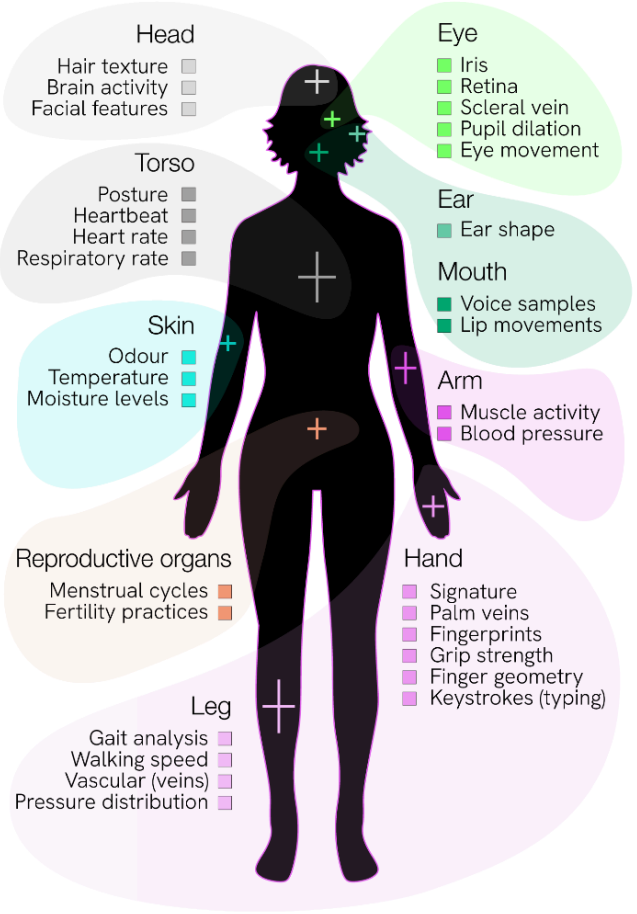
The primary **focus of this chapter is on three key areas of body-focused data collection: Electronic Health Record systems (EHRs), mobile health (mHealth) solutions, and biometric data collection**. We chose these three domains because they represent **centralized avenues for bodily data collection that focus specifically on the human body, offering insights into both physiological and mental health**, while also acknowledging that these are not the only domains where data-driven technological solutions have a profound impact on the human body. These domains use advanced technologies to facilitate continuous and precise data collection, allowing for real-time monitoring of bodily metrics and behaviors. Additionally, these three areas exemplify how new technologies mediate our relationship with our own bodies, reshaping our understanding of identity, wellness, and self-management in a digitized environment.

We will investigate how the landscape of these domains has evolved, the growth patterns within these sectors, as well as the implications of emerging AI tools in the context of body-focused data collection. Next, we turn our attention to the associated harms that arise from body-focused data collection in these three domains. The harms we analyze can manifest in various ways, including cyber extortion, data misuse, biometric persecution, or discrimination. Lastly, since effective legal protections are crucial for ensuring the privacy and security of bodily data, we will systematically review current regulations and identify shortcomings, with a focus on how emerging technologies may outstrip existing

legal frameworks. We primarily concentrate on the regulatory landscapes of the European Union and the United States due to the heightened regulatory discourse and legislative efforts in these regions, as well as their differing approaches to data privacy and protection.

AVENUES OF BODILY DATA COLLECTION

Physical traits and body parts



Behavioral, lifestyle and clinical metrics

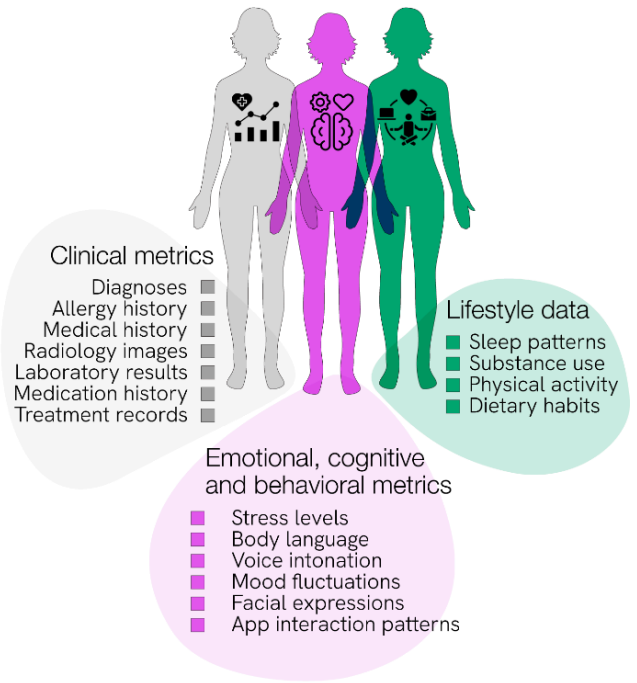


Table: Key avenues of body-focused data collection

Body parts		
Data type	Characteristics	Entities collecting
Overall body composition	**BMI**	Mobile health industry, EHR systems, biometric firms , research organizations
	Body fat	Mobile health industry, EHR systems, research organizations
	DNA information	Genetic testing labs, health clinics, biometrics firms, security firms
Head	**Brain activity**	EHR systems, biometric firms, genetic testing companies, medical device producers, neuroscience and research companies, mobile health apps
	Facial features	Biometric firms, security firms, consumer electronics companies, health monitoring companies, extended reality (XR) applications
	Hair texture	Beauty and personal care products, health and dermatology companies, cosmetic and hair styling firms
Torso	**Heart rate**	Mobile health industry, wearables manufacturers, fitness technology firms, extended reality (XR) applications
	Heartbeat	Medical device producers, mobile health industry, telemedicine providers
	Respiratory rate	Mobile health industry, tech firms, fitness tracking companies
	Posture	Mobile health industry, tech firms, ergonomic research firms
Eye	**Eye movement**	Mobile health industry, biometric firms, assistive technology firms, extended reality (XR) applications, security firms, research companies
	Retina	Biometric firms, eye clinics, telecommunications companies, health technology firms
	Iris	Biometric firms, security firms, mobile devices manufacturers
	Scleral vein	Research institutions, biometric firms, medical imaging companies
	Pupil dilation	Mobile health industry, extended reality (XR) applications, medical device producers, security firms, emotion recognition companies
Ear	**Ear shape**	Biometric firms, hearing aid manufacturers, security firms
Mouth	**Voice samples**	Mobile health industry, biometric firms, speech therapy firms, security firms, telecom companies, extended reality (XR) applications
	Lip movements	Biometric firms, speech therapy firms, security firms, telecom companies, extended reality (XR) applications
Arm	**Muscle activity**	EHR systems, mobile health industry, tech firms, rehabilitation centers
	Blood pressure	EHR, mobile health industry, tech firms, medical device manufacturers
Hand	**Grip strength**	Biometric firms, tech firms, rehabilitation centers
	Fingerprints	Biometric firms, security firms, mobile device manufacturers, government agencies
	Finger geometry	Biometric firms, security firms
	Palm veins	Biometric firms, security firms, financial institutions
	Keystrokes (typing)	Biometric firms, software developers, security firms
	Signature	Biometric firms, security firms, financial institutions
Leg	**Gait analysis**	Research institutions, biometric firms, rehabilitation facilities, security firms
	Vascular (veins)	Healthcare providers, medical imaging companies, research institutions, biometric firms

	Pressure distribution	Mobile health industry, EHR systems, orthopedic clinics
	Walking speed	Mobile health industry, fitness technology firms, research institutions
Skin	**Moisture levels**	Mobile health industry, EHR systems, tech firms, skincare companies, biometric firms
	Temperature	Mobile health industry, tech firms, medical device producers, biometric firms
	Odour	Biometric firms
Reproductive organs	**Menstrual cycles**	Mobile health industry, reproductive health apps, health clinics
	Fertility practices	Mobile health industry, reproductive health apps, fertility treatment centers, wellness apps
Clinical metrics		
Medical history	EHR, healthcare providers, insurance companies	
Diagnoses	EHR, healthcare providers, medical research institutions	
Treatment records	EHR, healthcare providers, clinical research companies	
Allergy history	EHR, healthcare providers, allergy clinics	
Medication history	EHR, healthcare providers, pharmacies	
Laboratory results	EHR, labs, hospitals, research institutions	
Radiology images	EHR, radiology clinics, hospitals, imaging centers	
Lifestyle data		
Physical activity levels	Mobile health industry, fitness companies, wearable tech firms	
Dietary habits, calorie intake	Mobile health industry, nutrition companies, fitness apps	
Sleep patterns	Mobile health industry, health monitoring devices, sleep clinics	
Substance use	Mobile health industry, addiction treatment centers, health services	
Emotional, cognitive and behavioral metrics		
Facial expressions	Biometric firms, mobile health industry, market research companies	
Body language	Tech firms, marketing agencies, behavioral research institutions	
Voice intonation	Biometric firms, communication technology firms, speech	
Stress levels	Mobile health industry, mental health apps, workplace wellness programs	
Mood fluctuations	Mobile health industry, mental health apps, research institutions, workplace monitoring programs	
App interaction patterns	App developers, mental health services, user experience researchers	

1.1. Electronic health record systems

1.1.1. Industry trends

EHR systems serve as centralized repositories for comprehensive health data, systematically capturing a wide range of information derived from medical care, including a patient's medical history, diagnoses, treatment records, medications, allergies, immunizations, radiology images, and laboratory results (Keshta and Odeh, 2020, Shah and Khan, 2020, Tertulino et al, 2023). Typically, health data from EHR systems is shared among medical service providers such as hospitals, general practitioners, pharmacies, and laboratories (WHO, 2015, OECD, 2021). In the past decade, **EHR systems have experienced steady growth across various care settings,** especially in medical specialist offices and hospital emergency departments (Ibid). The market was estimated between USD 26 and 34 billion, and is expected to reach approximately USD 45 billion by 2032, growing at a compound annual growth rate (CAGR) of around 7% (Grand View Research, 2024, Precedence Research, 2024, Fortune Business Insights, 2024, Global Market Insights, 2024).

In the United States, EHR adoption has been increasing steadily, largely due to regulatory initiatives such as the Health Information Technology for Economic and Clinical Health (HITECH) Act from 2009, which incentivized healthcare providers to replace paper records with electronic systems (Adler-Milstein and Jha, 2017). The market for EHR systems in the US alone is projected to grow from USD 8.46 billion in 2023 reflecting a significant push for optimized care coordination and enhanced patient engagement (Precedence Research, 2024). Similarly, in the European Union, the EHR market is also poised for growth, spurred by initiatives like the Health Data Space (EHDS), which aims to improve cross-border patient care and collaboration among healthcare providers (Bincoletto, 2020, Bak et al, 2022, Van Kessel et al, 2023, Raab et al, 2023), as described in further detail below.

Key players in the EHR industry include AdvancedMD, Allscripts, Athenahealth, CareCloud, Cerner Corporation (Oracle), CPSI, CureMD Healthcare, eClinicalWorks, Epic Systems Corporation, GE Healthcare, Greenway Health, LLC, McKesson Corporation, Medical Information Technology (MEDITECH), Modernizing Medicine, NextGen Healthcare, and Teladoc Health. These **organizations are pushing for new markets through product innovation such as launching advanced technologies like AI and cloud-based EHR systems, allowing for remote access and improved functionality** (Grand View Research, 2024, Precedence Research, 2024, Fortune Business Insights, 2024, Global Market Insights, 2024). They are engaging in geographic expansion by establishing a presence in emerging markets, as seen with Greenway Health's office in Bengaluru, India, while collaborations with government initiatives, such as compliance with the HITECH Act in the US and participation in European digital health initiatives, are also driving market growth (Ibid.). Additionally, mergers and acquisitions, such as Thoma Bravo's acquisition of NextGen Healthcare, are increasingly used to strengthen market position and expand product portfolios (Ibid).

The advancement of AI technologies has had a particularly profound impact on the market EHR solutions. **For public health record systems, AI tools promise better automation** (Falcetta et al, 2023), **improved analytical capabilities** (Calduch et al, 2021), and **enhanced diagnostic accuracy** (Lewis et al, 2023, Ozonze et al, 2023, Hossain et al, 2023). For example, AI-powered predictive analytics are increasingly deployed to analyze historical patient data to forecast trends such as anticipated patient admissions, with the promise of enabling healthcare

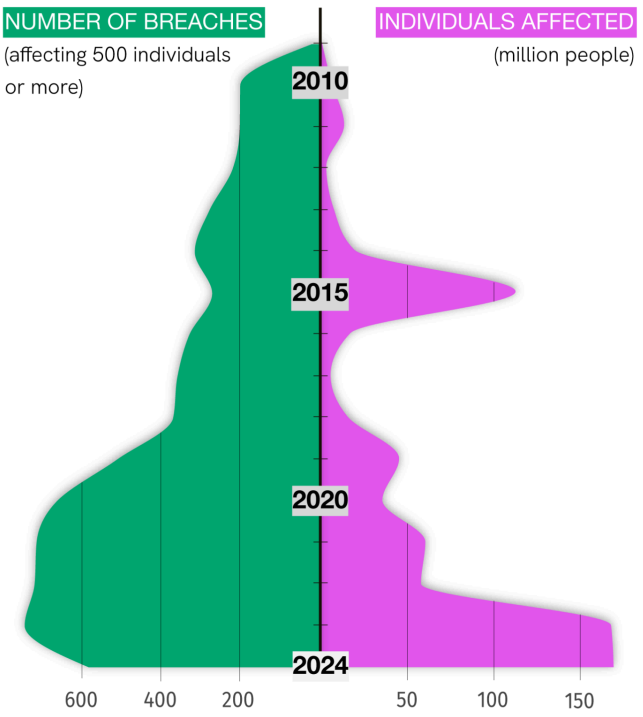
facilities to manage their resources more effectively (Hossain et al, 2023). In addition, AI is enhancing clinical workflows by automating routine administrative tasks such as data entry, coding, and appointment scheduling (Falcetta et al). The ability of AI algorithms to learn from existing data empowers clinical staff by providing decision support and alerts for potential health issues, with the promise of enhancing diagnostic accuracy (Lewis et al, 2023). Consequently, the growing demand for EHR systems that incorporate these AI capabilities is driving significant market expansion (Grand View Research, 2024, Precedence Research, 2024, Fortune Business Insights, 2024, Global Market Insights, 2024).

1.1.2. Data harms

With regards to data harms, **cybersecurity stands out as the most pressing concern for EHR systems, especially in light of the significant rise in cybercrimes** targeting sensitive patient information (Shah and Khan, 2020). Between 2009 and 2023, the HIPAA Journal reported 5,887 large healthcare data breaches in the United States, a rise attributed to escalating hacking and ransomware incidents (HIPAA, 2024). In fact, the number of breaches jumped dramatically from just 18 incidents in 2009 to 745 in 2023, highlighting the growing vulnerability of healthcare systems. In a similar vein, the European Union Agency for Cybersecurity (ENISA) recorded 215 healthcare-focused cybersecurity incidents on the continent from 2021 to 2023 (ENISA, 2023). These breaches not only cause substantial financial loss for healthcare providers (Basil et al, 2022), they can also disrupt medical services on a massive scale, as witnessed in Ireland in 2021, where healthcare institutions across the country were paralyzed after a massive online extortion campaign (Perlroth and Satariano, 2021).

Health data is also increasingly targeted for cyber extortion where hackers gain access to sensitive patient information and demand a ransom for its return or to prevent its public release. This form of cybercrime disrupts healthcare services and compromises patient confidentiality while imposing significant financial burdens on healthcare organizations that may have to invest in security measures or pay ransoms (Niki et al, 2022, Javaid et al, 2023). Furthermore, leaked health data can lead to discrimination and stigmatization, particularly impacting individuals with pre-existing medical conditions, who may face increased insurance premiums as insurers adjust pricing to account for heightened risk (Allen, 2018). Such data frequently makes its way onto the dark web, where it can be sold and resold indefinitely, exacerbating the vulnerabilities associated with identity theft and exploitation (Patterson and Kates, 2019).

RISING HEALTHCARE BREACHES IN THE US
2009-2024



data: US Department of Health and Human Services

Questions around security and privacy are only going to become more profound with the growing demand for interoperability, defined as the seamless exchange of health information across platforms and jurisdictions (Van Kessel et al, 2023, Raab et al, 2023). The push for interoperability is driven by motives like improving cross-border patient care or conducting nuanced clinical research (Ibid). Initiatives like the European Union's above mentioned EHDS (European Commission, 2022), while ambitious in scope, pose significant challenges for data protection, thanks to the increased opportunities for misuse and the growing complexity of managing patient consent in a cross-border data environment (Bak et al, 2022, Bincoletto, 2020). Some argue that the EHDS offers the technology industry an unprecedented opportunity to expand its influence over healthcare providers, governments and patients, and to increase its already significant market power (Schipper et al, 2024).

The integration of AI-driven tools into EHR systems also presents significant challenges. The **data-intensive nature of AI models contrasts sharply with existing privacy frameworks** that emphasize data minimization (Sorell et al, 2020), as AI technologies increase the potential for re-identification by revealing patterns that can reconstruct individuals' identities from anonymized data (Williamson et al, 2024). Additionally, the effectiveness of these tools is heavily reliant on the quality of their underlying algorithms and training datasets, which can lead to **biased and discriminatory outcomes** (Stark et al, 2021, Wen et al, 2022). For instance, AI systems used for diagnosing skin cancer are often trained on images of lighter-skinned patients, resulting in lower diagnostic accuracy for individuals with darker skin (Wen et al, 2022), while other studies confirm that disparities in access and health outcomes are significantly influenced by factors such as age, race, and socioeconomic status (Yao et al, 2022). These challenges are further compounded by concerns over accountability and transparency, as even healthcare providers may find it difficult to understand the formulation of AI-generated recommendations, commonly referred to as the 'black box' problem (Sorell et al, 2020, Calduch et al, 2021). Data quality issues are critical and pertinent in the context of AI in EHRs for several reasons. Firstly, high-quality data is fundamental for AI algorithms to make accurate and reliable predictions (Hossain et al, 2023); **flawed datasets can significantly degrade algorithm performance, leading to incorrect decisions.** Research indicates that many EHR systems often suffer from issues such as incompleteness, inaccuracies, and inconsistencies, which not only hinder effective patient care but also compromise the integrity of AI applications (Lewis et al, 2023, Ozonze et al, 2023). Furthermore, many existing EHR systems lack compatibility with one another, complicating the seamless exchange of information between organizations (Calduch et al, 2021, Falcetta et al, 2023).

1.1.3. Legal protections

In the European Union, the GDPR is the primary legislative avenue that governs health-focused data collection (General Data Protection Regulation, 2016). Health-related information is regarded as special category data, with strict limitations on sharing and processing (Carmi et al, 2022, Galetsi et al, 2023). This means that **EHRs in the EU must comply with stringent consent requirements and data handling practices,** ensuring that individuals' health information is only used for clearly specified purposes and with explicit user consent. The framework emphasizes the principle of "privacy by design," requiring that data protection measures are integrated from the outset of system development. Despite its robust framework for data protection, the GDPR faces significant gaps and challenges. Ambiguity in its language often creates uncertainty in

compliance, with **varying interpretations across EU member states leading to inconsistent enforcement** (Presthus and Sønslien, 2021, Bakare et al, 2024). The extensive documentation and processes required for compliance can overwhelm organizations (Presthus and Sønslien, 2021, Gentile and Lynskey, 2022, Bakare et al, 2024); and while the GDPR imposes significant penalties for non-compliance, the fines imposed by national data protection authorities across Europe vary significantly (Presthus and Sønslien, 2021, Ruohonen and Hjerppe, 2021). Additionally, the rapid advancement of data-driven technologies, especially AI tools, create significant challenges for the GDPR's consent framework, as these technologies can lead to continuous data processing without clear user awareness (Blanke, 2020, van de Waerdt, 2020).

The **EU's new AI Act, which aims to regulate artificial intelligence technologies across various sectors, has significant implications for EHR systems**. Firstly, the Act categorizes AI systems based on their risk levels, with high-risk AI applications—such as those used in healthcare for diagnosis or treatment planning—subject to stringent requirements (Minssen et al, 2024, Schmidt et al, 2024, Palaniappan et al, 2024). This includes mandatory risk assessments, documentation, and adherence to data governance principles, which directly impact how EHR systems employ AI functionalities for tasks like predictive analytics or clinical decision support.

Additionally, EHR systems utilizing AI tools will need to ensure compliance with transparency obligations, requiring healthcare providers to disclose when an AI system is being used to inform medical decisions, and to do so in easy-to-understand language (Schmidt et al, 2024, Williamson, 2024). Moreover, the AI Act emphasizes the importance of data quality and representativeness, mandating that training datasets for high-risk AI systems be adequate and suitable, which will necessitate healthcare organizations to invest in data management practices that enhance the quality and diversity of the data used in EHR systems (Minssen et al, 2024, Schmidt et al, 2024, Palaniappan et al, 2024).

The regulation of bodily and health data in the United States primarily falls under the Health Insurance Portability and Accountability Act of 1996 (Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC), which establishes strict standards for safeguarding health information created, received, or maintained by "covered entities," including hospitals, physicians, nursing homes, clinics, dentists, pharmacies, and other health service providers (Kaplan, 2020, Basil et al, 2022, Tertulino et al, 2023). **HIPAA in the US mandates that EHRs must ensure the confidentiality, integrity, and availability of protected health information**, creating a framework that compels healthcare organizations to implement robust administrative, physical, and technical safeguards. The previously mentioned HITECH Act of 2009 strengthened HIPAA's provisions by promoting the meaningful use of electronic health records, increasing penalties for HIPAA violations, and expanding the scope of patient privacy protections (HIPAA Journal, 2024).

HIPAA faces several significant challenges that hinder its effectiveness in successfully protecting health data. Firstly, its limited scope primarily addresses individually identifiable health information, leaving broader datasets that could impact patient privacy (like aggregate health data, anonymized information, or datasets from third parties) inadequately covered (Tertulino et al., 2023). HIPAA's consent process is rather cumbersome, often failing to ensure that patients fully understand how their data will be utilized or shared (Kaplan, 2021). There's also a lack of clarity within the guidelines regarding data-sharing practices, which can create confusion patients and providers about what is permissible under the law (Ibid). Enforcement mechanisms are

also regarded as rather fragmented, leading to inconsistent compliance among healthcare organizations (Nema & Sinha, 2024). Furthermore, the rapid evolution of emerging technologies make it difficult for the legislation to keep up-to-date, especially with the rise of third-party applications and platforms for health data management, as described in the next chapter (Tertulino et al., 2023, Nema & Sinha, 2024).

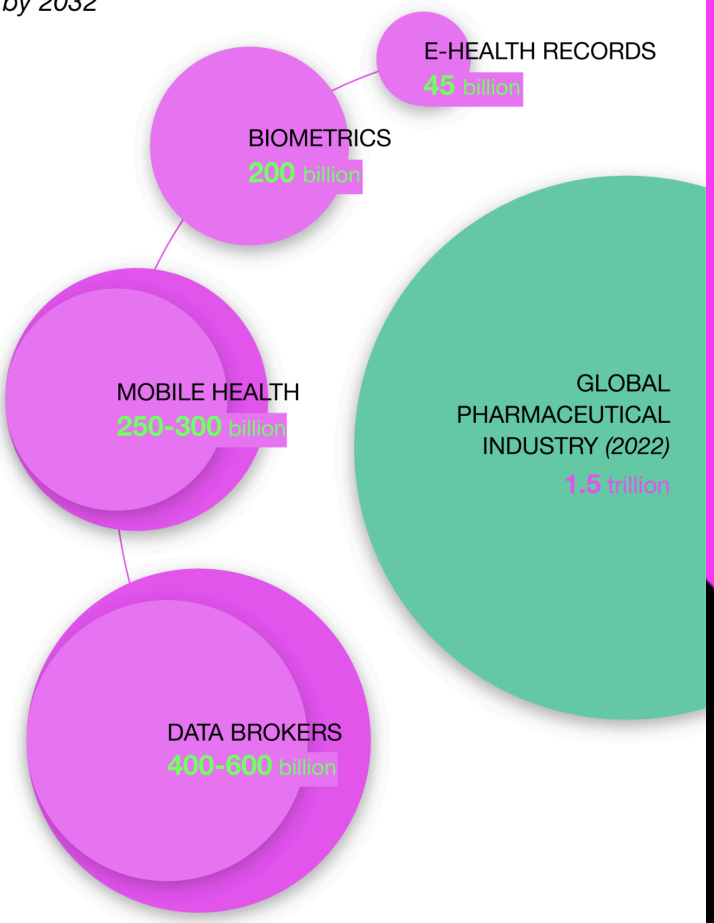
1.2. Mobile health solutions

1.2.1. Industry trends

Mobile health technologies **enable real-time data collection through mobile applications and wearable devices, facilitating insight into personal behaviors and physiological metrics**. These apps and wearable devices are primarily designed to enhance fitness and health regimens, or to support remote patient monitoring. Fitness and mental health applications can access a diverse range of bodily data, including workout routines, sleep patterns, calorie intake, menstrual cycles, fertility practices, blood pressure, health conditions, as well as data on mood fluctuations, depression, teletherapy services, and substance abuse patterns (Tangari et al, 2021, Wang et al, 2021, Amagai et al, 2022, Van Kessel, 2023, Omaghomi et al, 2024).

The mobile health industry has **experienced significant growth during the COVID-19 pandemic**, a trend that has continued ever since (Wang et al, 2021, Amagai et al, 2022, Van Kessel, 2023). The global mobile healthmarket, valued at approximately USD 100 billion in 2022, is projected to reach around USD 250-350 billion by 2032, growing at a CAGR of approximately 13-15% (Grand View Research, 2024, Fortune Business Insights, 2024, Precedence Research, 2024, Transparency Market Research, 2024). Key players like Apple, AT&T Intellectual Property, Bayer Healthcare, Cisco, Dexcom, Fitbit, Google, Johnson & Johnson, Koninklijke Philips, Masimo, Medtronic, Omron, Orange, Qualcomm, Samsung, Sanofi, SeekMed, SoftServe, Telefonica, Veradigm and Vodafone, are innovating with product launches that include new applications and wearable devices (Ibid). These companies are also engaging in mergers and acquisitions to enhance their offerings and expand geographically, particularly in emerging markets like the Asia-Pacific. Collaborative initiatives between technology firms and healthcare providers are also prevalent, aiming to integrate mobile health solutions with existing EHR systems to improve service delivery (Ibid).

PROJECTED GROWTH OF KEY INDUSTRIES
by 2032



data: market research companies

Similarly to EHR solutions, the mobile health industry has experienced a significant boost thanks to the **spread of AI models that create personalized recommendations and predict future potential health outcomes** (Khan et al, 2020, Galetsi et al, 2022, Deniz-Garcia et al, 2023). To illustrate, predictive models on the market promise to help analyze data from wearable devices, such as heart rate monitors and smartwatches, along with patient-reported metrics to identify early warning signs of heart failure (Khan et al, 2020). By detecting variables like increased heart rate, elevated blood pressure, or rapid weight gain, these models can generate alerts for patients and healthcare providers alike.

AI tools have a **particularly profound impact on mental health apps, by promising more accessible care, real-time emotional support, and immediate crisis detection** (Khan et al, 2020, Hamdoun et al, 2023, Olawade et al, 2024). For instance, some apps utilize AI-driven chatbots to engage users in therapeutic conversations or to deliver certain therapy methods, such as Cognitive Behavioral Therapy (CBT) (Oh et al, 2020, Jang et al, 2021), while others leverage AI for mood tracking and complex analysis, or deploy predictive analytics tools to assess the likelihood of mental health-related incidents. (D'Alfonso, 2020, Olawade et al, 2024). In crisis scenarios, text support services like Crisis Text Line use AI to analyze incoming messages for urgency, enabling triaging between trained counselors and providing automated initial responses (Szlyk et al, 2021).

1.2.2. Data harms

The key harms associated with the mobile health industry revolve around security breaches, data misuse, algorithmic bias, and harmful health interventions due to a lack of proper regulation and oversight. To illustrate, a 2017 breach of data collected by MyFitnessPal compromised the sensitive information of approximately 150 million users (Masuch et al, 2021, Aswathi et al, 2022), while a database holding over 61 million records—including health-related data from wearable technologies and fitness services like Fitbit and Apple HealthKit—was found unsecured in 2021 (Fowler, 2021). A 2020 investigation revealed vulnerabilities to cyberattacks across all leading mobile health apps (Knight, 2020), and a 2022 research from Dhondt et al found that popular fitness trackers often leaked location data, even when users had established privacy zones within the app settings (Dhondt et al, 2022). Iwaya et al revealed significant data privacy issues in mental health apps, including unnecessary permissions, insecure data handling and transmission, high risks of user profiling due to linkability and identifiability threats, and inadequate transparency in privacy policies (Iwaya et al, 2022). And while exact statistics on cybersecurity breaches within the mobile health industry are not readily available, these tools are particularly susceptible to spyware and malware attacks (malicious software that targets patient data), encryption vulnerabilities, man-in-the-middle attacks (gathering data from individual patients through, for instance, fraudulent WiFi access points), and poor code protection (weak safeguards that allow attackers to extract information) (Diamant, 2022).

Unlike EHR systems which are subject to strict regulations, the mobile health industry faces significant challenges related to data misuse; particularly in the US, where a lack of stringent legal protections has resulted in vague and ambiguous privacy policies and opaque data handling practices (Tangari et al, 2021, Iwaya et al, 2022, Saha, 2023). Consequently, several health and mental health apps like Talkspace and Crisis Text Line have been sharing sensitive patient conversations with researchers, advertisers and data brokers without explicit user consent, resulting in significant public outcry (Hill and Krolik, 2020, Hendel, 2022). A report by Mozilla

highlighted that romantic AI chatbots compromise user privacy and often exploit personal data while masquerading as supportive companions (Caltrider et al, 2024). The harmful implications of non-consensual data sharing can be particularly severe in sensitive contexts, such as for reproductive health apps, which have been known to share intimate data without obtaining explicit user consent (Shipp et al, 2020, Healy, 2020, Mehrnezhad and Almeida, 2021, Alfawzan et al, 2022, Purdon, 2023). The controversy surrounding the menstrual tracking app Flo, a period tracker that shared sensitive data with third-party companies like Facebook, illustrates how such misuse could lead to discrimination, stigmatization, or even legal repercussions in states or countries with restrictive reproductive laws (International Association of Privacy Professionals, 2024).

In addition to concerns regarding data security and privacy, some other critical issues surrounding mobile health applications deserve attention. This includes the **uncertainty regarding the overall effectiveness of these novel tools, as existing research often lacks rigorous evaluation and empirical evidence to substantiate claims of efficacy** (Grundy, 2022, Rossmaier et al, 2023). The effectiveness of these apps are particularly limited by their reliance on commercial ecosystems, which prioritize profit over public health benefits (Tarricone et al, 2021, Grundy, 2022). The **unreliability of these tools is particularly problematic for mental health apps, where the nuances of psychological conditions necessitate validated interventions that are sensitive to individual needs** (Silk et al, 2019, Oh et al, 2020). The risk of overreliance on mobile health apps exacerbates these concerns, as users may substitute digital solutions for essential, in-person consultations with healthcare professionals (Silk et al, 2019, D'Alfonso, 2020, Oh et al, 2020, Jang et al, 2021, Olawade et al, 2024). The tragic case of a Belgian man who took his own life after being encouraged to do so by an AI chatbot highlights these risks (Xiang, 2023), underscoring that computational models inherently lack the empathy necessary for delivering effective emotional support and may struggle to recognize certain critical crisis moments (Haque and Rubya, 2023, Olawade et al, 2024).

Many of the above described challenges related to the integration of AI-driven tools into EHR systems also apply to the mobile health industry, particularly concerning data privacy, the risk of re-identification, the reliance on high-quality datasets for accurate health assessments, and potential biases from flawed algorithms and training datasets (Callier and Fullerton, 2020, Grundy, 2022, Olawade et al, 2024). Unlike EHR systems, which are primarily utilized by healthcare professionals, mobile health solutions are often used by individuals for health interventions without direct medical oversight. This **lack of control makes inaccuracies in recommendations even more dangerous, as users may take actions based on unreliable or misleading information**. Cultural differences are also often overlooked in AI models, especially given that racial and ethnic minorities are significantly underrepresented in biomedical research, resulting in particularly ineffective and potentially even harmful health recommendations for marginalized communities (Callier and Fullerton, 2020, Olawade et al, 2024).

1.2.3. Legal protections

With regard to legal protections, the GDPR remains the key instrument to govern the mobile health industry in the European Union. One of the most crucial elements of the GDPR for the mobile health market is the "privacy by design" principle which requires that privacy is incorporated as early as the development stage of platforms and apps that handle health data, mandating also that such data can only be gathered for certain purposes and with explicit and informed user consent (Martinez et al, 2023). **The GDPR is further supported by the Privacy Code**

of Conduct on Mobile HealthApps, created by the European Commission in collaboration with industry partners to offer practical guidelines for the mobile health industry (European Commission, 2018). Similarly to EHR systems, the **EU's new AI Act will shape the integration of AI models into mobile health apps, particularly around risk classification**, which will impose stringent requirements on high-risk applications used for health monitoring and decision making; ensuring transparency in how AI influences health recommendations and user interactions; and enforcing data governance standards that mandate the collection and use of high-quality, representative datasets to prevent biases and ensure accurate health assessments for diverse populations (Minssen et al, 2024, Schmidt et al, 2024, Palaniappan et al, 2024, Williamson, 2024).

Other **relevant regulatory efforts for the European Mobile Healthmarket include the Digital Services Act (DSA, 2022) and the Digital Markets Act (DMA, 2022)**, both of which entered into force in late 2023. While the DMA aims to increase competition in European markets by preventing large digital platforms from abusing their market power, the DSA focuses on platform liability and transparency, covering a wide range of areas from content moderation, to online advertising and algorithmic transparency, to disinformation (Duivenvoorde et al, 2023, Farinho, 2023, Chiarella, 2023, Botta and Borges, 2023). And while it's still a relatively new framework, the DSA is of particular importance in the context of data privacy, including provisions that limit the use of targeted advertising based on sensitive attributes. This includes targeted advertising directed at minors, as well as targeting based on religion, sexual orientation, health, ethnicity or political affiliation (Ibid).

In the US, while the HIPAA provides a foundational legal framework governing how healthcare providers process patient data through EHR systems, the regulatory landscape for mobile health solutions is more complicated. This complexity arises primarily because many **mobile health apps centered on wellness, fitness, or lifestyle management fall outside the purview of HIPAA regulations** due to their lack of integration into traditional healthcare frameworks (Galetsi et al, 2023, Saha, 2023). Consequently, these apps may not be held to the same stringent standards that protect patient health information, leaving users' data potentially exposed.

For mobile health applications that specifically qualify as medical devices—such as diabetes management apps or applications aimed at managing chronic diseases—there is an additional layer of oversight mandated by the Food and Drug Administration (FDA). These **medical applications are required to meet rigorous standards for safety and efficacy**, reflecting their critical role in health management and the potential implications for patient safety (Ibid).

This regulatory distinction highlights the necessity for developers of mobile health apps to navigate diverse regulatory requirements depending on the classification of their applications. Moreover, the Federal Trade Commission (FTC) plays a significant role in overseeing the collection of health-related data in the US, but its regulatory focus tends to lean more towards preventing deceptive practices in commercial activities rather than enforcing comprehensive data privacy policies. This results in modest protections for consumer data and can leave gaps in oversight regarding how personal health information is collected, used, and shared (Hanus, 2024, Kovacic, 2024). Additionally, most recent changes to the FTC's Health Breach Notification Rule (HBNR) require certain entities that collect health-related information to notify consumers about data breaches, thus providing some level of accountability in the space (Federal Trade Commission, 2024).

1.3. Biometric techniques

1.3.1. Industry trends

Biometric data collection exemplifies how body-focused data collection intersects with cutting-edge technological innovation. These technologies are developed with the aim of identifying, verifying, and in some cases, classifying people based on their unique bodily and behavioral characteristics (Awad et al, 2024, Marani et al, 2023, Fortmeyer, 2024). In the past decade, this primarily happened through fingerprint recognition, facial recognition and voice recognition. However in recent years the scope of the industry has expanded with the emergence of innovative techniques like gait analysis, that measures an individual's walking pattern to confirm their identity, or odor recognition, that uses people's unique scent profile for identification (Marani et al, 2023, Perosa and Tsui, 2023, Lucia et al, 2023 Fortmeyer, 2024, Ayeswarya et al, 2024). Additionally, advancements in genomic and genetic (including DNA) testing techniques have also enabled more accurate identification, increasingly used in commercial applications such as paternity testing or ancestry services, and other avenues like healthcare or forensic investigations (Bonomi et al, 2020, Wan et al, 2022). Similar to other examined avenues of body-focused data collection, the **biometric industry has witnessed substantial growth over the past decade** and is now mainstream across various industries, including finance and banking (Marani et al, 2023), healthcare (Lucia et al, 2023, Sardar et al, 2023), and law enforcement (Fabrègue et al, 2023). Smart home and vehicle technologies also routinely collect biometric data, in order to be able to analyze personal interactions and household habits (Popoola et al, 2023, Rao and Debaak, 2022, Singhai et al, 2021). Market projections for the global biometrics industry vary widely but even the more conservative estimates expect the sector to grow to approximately USD 100 billion by 2030 and above 200 billion by 2032, with a CAGR of around 15-20% (Grand View Research, 2023, IMARC Group, 2024, Markets and Markets, 2024).

Key players in the biometric sector include companies like Accu-Time Systems, AFIX Technologies, BIO-Key International, DERMALOG, East Shore Technologies, EyeVerify, Fujitsu Limited, Gemalto NV, HID Global Corporation, IDEMIA, Iris ID, NEC Corporation, RCG Holdings, Siemens AG, Suprema, Thales, and 3M Cogent. These groups are driving new market opportunities through product innovation, such as the development of advanced biometric authentication technologies, including AI-enhanced systems (Grand View Research, 2023, IMARC Group, 2024, Markets and Markets, 2024). Leading biometrics companies are pursuing geographic expansion by entering emerging markets, as demonstrated by MasterCard's introduction of biometric payment cards in the Middle East and Africa, while **partnerships with governments, such as initiatives to enhance border security using biometric systems, are also propelling growth for the sector** (Ibid). In fact, biometric data is increasingly harnessed by law enforcement and border control agencies, child protective services, and humanitarian organizations (Church et al, 2017, Molnar, 2022, Westlake et al, 2022, Perosa and Tsui, 2023). Furthermore, mergers and acquisitions, like Thales Group's acquisition of AVI-SPL, are increasingly employed to strengthen market positions and diversify product portfolios (Grand View Research, 2023, IMARC Group, 2024, Markets and Markets, 2024).

In the biometrics industry, the greatest promise of Artificial Intelligence tools lies in the possibility for improved accuracy, more reliable identification systems and a better integration of various biometric modalities (Lagerkvist et al, 2022, Awad et al, 2024,

Hussain et al, 2023). Increasingly, AI models are also being deployed to analyze unique user patterns and behaviors like mouse movements or typing speed, called "behavioral biometrics" (Tran et al, 2021, Sharma and Elmiligi, 2022, Baig et al, 2023, Killoran et al, 2023). Unlike traditional biometrics, which rely on physical traits, **behavioral biometrics analyze patterns in human behavior, such as typing dynamics or mouse movements** (Tran et al, 2021, Sharma and Elmiligi, 2022). These methods are increasingly used for "continuous authentication" processes where users' activities are monitored throughout entire sessions rather than at a single login point (Ibid). Another related area is **emotion recognition, a set of technologies that aim to evaluate and interpret human emotional states from facial expressions, voice intonations, body language, and even skin changes,** employing methods such as questionnaires, physical signals, and physiological signals like electrocardiography (ECG), galvanic skin response (GSR), and eye tracking (Alswaidan and Menai, 2020, Akhand et al, 2021, Khare et al, 2023, Zhang et al, 2023). Emotion recognition has applications across multiple fields, including healthcare, affective computing, human-robot interactions, market research and recruitment (Ibid).

1.3.2. Data harms

Regarding the data harms associated with biometric systems, numerous examples exist. **Data breaches and inappropriate data handling are serious and growing concerns**, akin to those faced in other areas such as EHRs and mobile health applications; however, biometric data is particularly sensitive because it is immutable and cannot be changed once compromised, making the potential for misuse and long-term consequences even more significant. Facial recognition company, Clearview AI, has been fined over USD 9.4 million by the UK's Information Commissioner's Office for the unauthorized collection of billions of facial images (Hart, 2022). In 2021, American donors in Afghanistan left behind biometric data after withdrawing from the country, which put locals working closely with US agencies in considerable danger after the Taliban takeover (Guo and Nori, 2021). The UN refugee agency (UNHCR) also received significant criticism for collecting biometric information from Rohingya refugees and sharing with the Bangladeshi government, jeopardizing their safety and security (Human Rights Watch, 2021). Additionally, genomics and biotechnology company, 23andMe, had shared genetic data from its users with pharmaceutical companies for research purposes without obtaining explicit consent, causing significant public outcry (Demopoulos, 2024).

Research has also consistently shown that **contemporary biometric systems exhibit significant biases and can lead to large-scale discrimination**. Buolamwini and Gebru revealed that facial recognition systems misidentified darker-skinned individuals at rates of up to 34% compared to less than 1% for lighter-skinned individuals (2018), leading to wrongful arrests and eroding public trust, as exemplified by the case of Williams v. City of Detroit, for instance (American Civil Liberties Union, 2024). The unreliability of these systems has contributed to a significant distrust among marginalized communities, as highlighted by a Pew Research Center survey indicating that many African American and Hispanic respondents were more wary of biometric technologies due to fears of misuse and discrimination. India's Aadhaar system, which saw serious data breaches (University of Washington, 2019), has also been criticized for causing confusion and exclusions in the public distribution system, preventing vulnerable individuals and families from accessing essential resources like food (The Wire Staff, 2018).

Concerns regarding the **validity of emotion recognition technologies have intensified with the**

industry's increasing reliance on AI techniques, particularly as these systems are collectively categorized under the broader umbrella of biometrics. Critics emphasize that many **applications of emotion recognition lack robust scientific foundations or rely on outdated psychological theories that overlook cultural differences, leading to incorrect conclusions, bias, and misinterpretation** (Barrett et al, 2019, Zhang et al, 2020, Flynn et al, 2020, Cabitza et al, 2022, Andrews, 2024). The issue becomes particularly pronounced when these technologies rely on single-modality datasets, such as facial expressions, which stem from the flawed assumption that all humans exhibit universal emotional expressions. This is especially concerning in high-stakes environments like law enforcement and hiring (Ibid), as these biases rooted in ableism further exacerbate the risks of unequal treatment for individuals whose emotional expressions may not conform to prevailing societal norms (Access Now, 2023). AI-powered recruitment algorithms reportedly introduce biases against individuals with disabilities by relying on criteria that do not accurately measure their job-related skills, such as optimism or emotional stability, exacerbating economic disparities for disabled job seekers (Center for Democracy and Technology, 2020).

In response to these challenges, **recent advancements aim to enhance the reliability of these techniques by incorporating insights from multiple psychology and neuroscience, and by prioritizing multi-modality datasets** like the combination of eye movement, facial expressions and breathing patterns, which provide a more comprehensive understanding of emotional expression (Alswaidan and Menai, 2020, Akhand et al, 2021 Zhang et al, 2023). However, as this technology becomes more advanced, a whole new set of questions arise regarding the privacy of human emotions and the extent to which emerging technologies can gain access to users' innermost feelings. Such questions become increasingly relevant as biometric technologies are at significant risk of "function creep," where tools developed for specific purposes, such as detecting mental distress or monitoring attention, are reallocated for use in areas like law enforcement as "AI lie detectors" (Access Now, 2023).

Lastly, it is essential to recognize that the **collection of bodily data transcends commercial interests and has significant implications for the relationship between the state and its citizens**. Governments are increasingly utilizing biometric data not only for traditional purposes such as population management and disease control, but also for more sophisticated applications enabled by AI. Government entities across the world have begun deploying predictive analytics and other advanced AI-driven tools to gain deeper insights into population behaviors, health trends, and socio-economic patterns (Angwin et al, 2016, Eubanks, 2017, Glaberson, 2019, Rahman and Keseru, 2021). This evolution raises serious concerns about the extent of state monitoring capabilities and the potential for future government surveillance practices.

1.3.3. Legal protections

While in the EU the **GDPR explicitly prohibits the processing of biometric information in certain cases, several exceptions exist for instances when such data collection is regarded as necessary for the public interest.** Since these exceptions are vaguely defined, significant regulatory gaps arise (Kindt, 2023, Tangerding, 2021). Furthermore, since the GDPR only classifies biometric data as special-category data when it is used to identify an individual, certain biometrics techniques like emotion recognition are subject to less stringent regulation. The EU's AI Act tries to address some of these concerns by introducing a risk-based approach to biometric identification systems. It also establishes more

nuanced compliance requirements while explicitly banning practices such as biometric surveillance in public spaces (the EU Artificial Intelligence Act, 2024). **Civil society organizations have, however, severely criticized the Act for its failure to effectively ban some of the most harmful instances of biometric data collection**, including mass surveillance or predictive policing, and for its failure to introduce meaningful transparency protocols (ProtectNotSurveil Coalition, 2024). Additionally, the Act includes prohibitions on cognitive behavioral manipulation and persuasion, which critics argue are too vague to effectively guard against these harms (Ibid).

As to biometric data, the **US regulatory environment lacks a comprehensive federal policy, creating significant regulatory gaps and loopholes** for organizations who handle such data without being subject to HIPAA (Mendolla, 2023). Certain states like Illinois have developed specific regulations governing biometric data handling (Biometric Information Privacy Act [BIPA]), with many other states following suit (Huddleston and Hedges, 2021). Furthermore, some cities in California, like San Francisco, and the state of Massachusetts, have instituted bans on facial recognition in law enforcement (Stop Secret Surveillance Ordinance, Commonwealth of Massachusetts, Bill S1385), but such regulation remains rare.

At the **intersection of data collection and human emotions, the "neurorights" movement has emerged, advocating for stronger protections related to the human brain** (Ienca, 2021, Douglas and Forsberg, 2021, Tesink et al, 2023). While this movement originated in response to advancements in neuroscience and the proliferation of brain-computer interfaces, it is increasingly framed within the context of privacy concerns and violations of freedom of thought attributed to the technology industry. Proponents of neurorights urge the establishment of new laws and policies to govern the collection, analysis, and application of data related to brain activity and cognitive functions. Recently, California introduced an amendment to the California Consumer Privacy Act (Senate Bill No. 1223, 2024), explicitly including neural data and recognizing the significance of mental privacy (Hamzelou, 2024). This legislation provides consumers with rights regarding the collection, sharing, and deletion of their brain data; however, critics have pointed out ambiguities in the protections concerning inferences drawn from such data (Ibid).

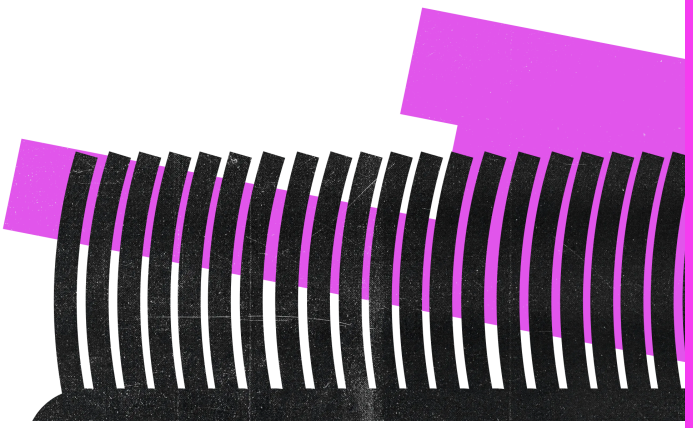
Table: Key industry trends for body-focused data collection

Category	Electronic health records	Mobile health	Biometrics
Projected growth	USD 26-34 billion to ~45 billion by 2032 (CAGR ~7%)	USD 100 billion to ~250-350 billion by 2032 (CAGR ~13-15)	~USD 100 billion by 2030 to >200 billion by 2032 (CAGR ~15-20%)
Key players	AdvancedMD, Allscripts, Athenahealth, CareCloud, Cerner Corporation (Oracle), CPSI, CureMD Healthcare, eClinicalWorks, Epic Systems Corporation, GE Healthcare, Greenway Health, LLC, McKesson Corporation, Medical Information Technology (MEDITECH), Modernizing Medicine, NextGen Healthcare, Teladoc Health.	Apple, AT&T Intellectual Property, Bayer Healthcare, Cisco, Dexcom, Fitbit, Google, Johnson & Johnson, Koninklijke Philips, Masimo, Medtronic, Omron, Orange, Qualcomm, Samsung, Sanofi, SeekMed, SoftServe, Telefonica, Veradigm, Vodafone.	Accu-Time Systems, AFIX Technologies, BIO-Key International, DERMALOG, East Shore Technologies, EyeVerify, Fujitsu Limited, Gemalto NV, HID Global Corporation, IDEMIA, Iris ID, NEC Corporation, RCG Holdings, Siemens AG, Suprema, Thales, 3M Cogent.
Market expansion strategies	Product innovations, such as AI and cloud-based EHR systems, predictive analytics tools for better clinical decision-making; mergers and acquisitions; geographic expansions; partnerships with healthcare providers.	Product innovations, such as new wearable devices, remote patient monitoring tools, predictive analytics tools, AI-powered chatbots; mergers and acquisitions; geographic expansions; partnerships with healthcare providers.	Product innovations, such as advanced biometric authentication technologies; mergers and acquisitions; geographic expansions; partnerships with governments, law enforcement, child protective and humanitarian agencies.
Promised benefits	Improved care coordination; better automation; enhancing clinical workflows; improved analytical capabilities; enhanced diagnostic accuracy; cross-border care coordination; enhanced patient engagement	Real-time patient monitoring; improved alert systems; personalized health insights into psychological and physiological metrics; enhanced fitness and health regimens; better predictions of future health outcomes; immediate crisis interventions; and real-time emotional support.	Enhanced accuracy in identification, verification, and classification; improved integration of diverse biometric modalities; more precise paternity testing and ancestry services; continuous authentication systems; better analysis of household habits; and improved recognition of human emotions and behaviors.
Key legislative avenues in the EU and the US	General Data Protection Regulation (GDPR, EU); EU Artificial Intelligence Act (EU); Health Insurance Portability and Accountability Act (HIPAA, US); Health Information Technology for Economic and Clinical Health Act (HITECH Act, US).	General Data Protection Regulation (GDPR, EU); Privacy Code of Conduct on Mobile Health Apps (EU); EU Artificial Intelligence Act (2024, EU); Digital Services Act (DSA, 2022, EU); Digital Markets Act (DMA, 2022, EU); Health Insurance Portability and Accountability Act (HIPAA, US); Food and Drug Administration (FDA, US); Federal Trade Commission (FTC, US). Senate Bill No. 1223 (2024, US, California).	General Data Protection Regulation (GDPR, EU); EU Artificial Intelligence Act (2024, EU); Biometric Information Privacy Act (BIPA, US, Illinois); Stop Secret Surveillance Ordinance (US, California); California Consumer Privacy Act (CCPA, US, California); Senate Bill No. 1223 (2024, US, California).

1.4. Other avenues of bodily data collection

While our research cannot cover every contemporary avenue of bodily data collection, it is essential to recognize the prevalence and implications of other technologies that rely heavily on body-focused data. For instance, **location tracking** technologies are increasingly deployed to gather insights into user movements and behavioral characteristics (Baron et al, 2021), across multiple sectors including marketing, urban planning, and public safety. The widespread use of **CCTV cameras** in public spaces further exemplifies the existing trend toward monitoring and analyzing bodily data in real-time. This is particularly evident in contexts such as education, where surveillance technologies are employed for safety and administrative purposes (Meishar-Tal et al, 2022, Beetham et al, 2022, Devkota et al, 2024), and in workplace monitoring, where employers may track employee activities to enhance productivity (Turanjanin, 2020, Swedish Commercial Employee's Union, 2022, Rehman, 2022). Such practices raise important questions about privacy and consent, particularly regarding how this data is handled and who has access to it.

Furthermore, **extended reality (XR) applications**, including virtual reality (VR) games and augmented reality (AR) solutions, capture significant amounts of bodily data. These technologies are capable of making sophisticated inferences about users' physical and mental states (Heller, 2023), enhancing user experience but also raising concerns about the implications of such intimate data collection. **Online search histories** represent another avenue through which a wealth of information about users' health-related interests and concerns can be gleaned (Bernal, 2015). Such data can reveal sensitive information about individuals' health behaviors, anxieties, and choices, contributing to a broader understanding of public health trends but also presenting significant privacy risks.



1.5. Linking it all together - the data broker industry

The rise of body-focused data collection across multiple domains has heightened **awareness of the inferences that can be drawn from seemingly innocent data points**, drawing increased attention to the evolving practices of the **data broker industry**. These companies are specialized in buying, selling and trading the data they collect from the internet, creating detailed consumer profiles for anyone with the necessary financial means to purchase them (Morrison, 2020, U.K. Information Commissioner's Office, 2020, Keagen and Eastwood, 2023, Armitage et al, 2023, Kanwal and Walby, 2024). To illustrate the magnitude of the problem, a 2023 report by Duke University revealed that data brokers were selling information identifying individuals based on mental health diagnoses, including depression, anxiety, and bipolar disorder, and while many deleted personal

identifiers, some continued to provide names and addresses of individuals seeking mental health assistance (Kim, 2023). And the data broker industry is projected to grow significantly, with estimates suggesting it could reach between $400 billion and $600 billion by the end of the decade (Markets Research Future, 2024, Knowledge Sourcing Intelligence, 2024, IndustryARC, 2024).

In order to achieve the most accurate results, data brokers **deploy a range of techniques to collect personal data, leveraging both direct and indirect sources**. As traditional third-party cookies are progressively being phased out, data brokers discover new methods to extract valuable information from existing data (UK Information Commissioner's Office, 2020, Wodinsky and Barr, 2022, Ruschemeier, 2023).

These include scraping publicly available records, such as electoral registers, census data, property and company records (Kanwal and Walby, 2024); purchasing data directly from companies, including retailers that sell customer shopping habits and browser histories (Lawson, 2023, Cox, 2024). Many mobile applications incorporate software development kits (SDKs) that enable them to access user permissions, including location, contacts, and usage data (Morrison, 2020, Armitage et al, 2023).

These SDKs often operate in the background and can facilitate extensive data collection, allowing developers to gather sensitive information without users' explicit knowledge. Consequently, apps can function as tools for rampant data collection, with permissions requested at installation often not clearly disclosed. Furthermore, mobile advertising IDs (MAIDs) link and profile individuals based on device data, enabling brokers to infer sensitive characteristics such as health status or lifestyle choices (Cox, 2022). However, MAIDs are also being phased out for this precise reason, with many companies making their mobile advertising IDs opt-in, a change that many users did not choose to comply with.

To further complicate matters, data brokers now **create complex user profiles by aggregating multiple data points**. Location data, for instance, can expose sophisticated insights about people's health status, through their visits to places like hospitals or abortion clinics (Smalley, 2024), and companies like Google have been reported to keep such data even after promising to delete it (Bhuiyan, 2024).

This has led many data brokers to shift their attention from raw data to aggregated insights, in order to gain new customers in various sectors such as advertising, insurance and pharmaceuticals, or even law enforcement (Armitage et al, 2023). As a result, the FTC has already started banning companies like X-Mode from selling location data that could be used to track people's visits to sensitive locations, including medical and reproductive health clinics (Federal Trade Commission, 2024). This is especially concerning given that this sensitive data often ends up on the dark web, where it can be exploited for malicious purposes, heightening the risk of identity theft and discrimination (Patterson and Kates, 2019).

The increasing capabilities of the data broker industry to harvest and analyze bodily data have heightened concerns about intrusive behavioral targeting practices. By categorizing individuals into various risk profiles, such as "likely pregnant" or "person with potential borderline disorder," data brokers enable companies to more precisely target vulnerable populations with their marketing strategies. For instance, individuals exhibiting online behaviors characteristic of at-risk gambling are increasingly targeted with ads for online gambling platforms (Guillou-Landreat et al, 2021).

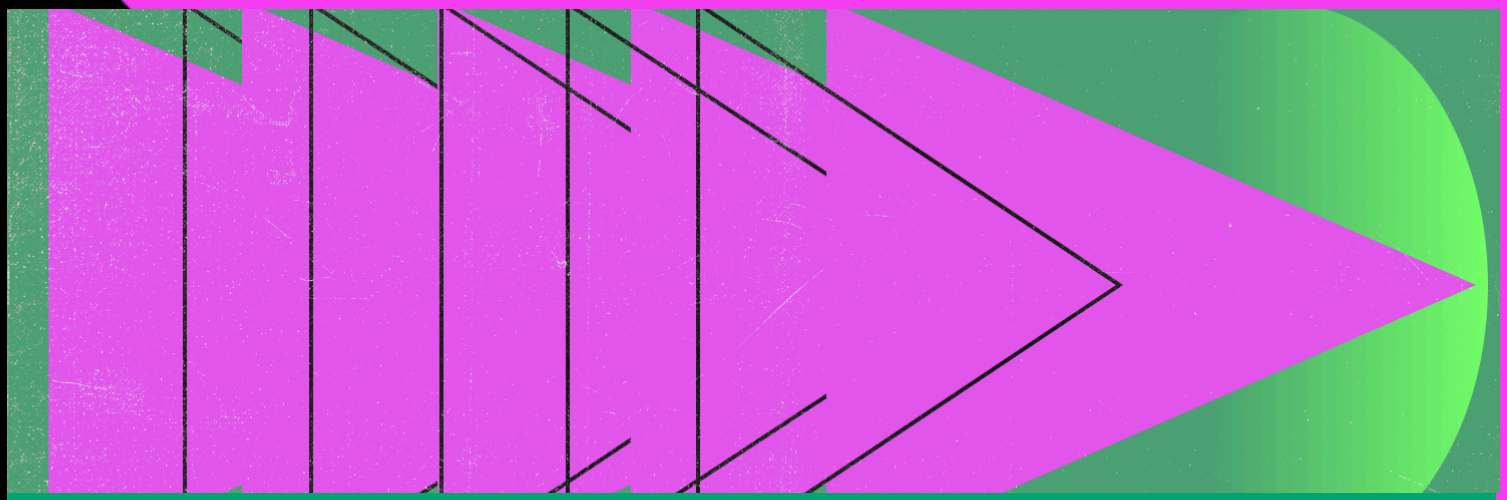
Meanwhile, women who may not want to disclose their pregnancies have been subjected to targeted advertising for pregnancy products based on early behavioral indicators gathered from data analytics (Hill, 2022).

With regards to legal protections, the EU governs data brokers through the same legal framework as mobile health apps and public health record systems, namely the GDPR, which mandates explicit user consent for any data collection and processing. However, data brokers often rely on previously granted permissions to justify their operations, and while EU citizens have the right to know how their data is used for secondary purposes, average users only have limited understanding of the intricacies of the data economy (Custers et al, 2022, Micheli et al, 2023). In contrast, **the regulation of data brokers in the US is marked by a lack of comprehensive federal standards,** creating a significant regulatory gap (Guay et al, 2022, Reviglio, 2022, Chong, 2023). This gap has been meticulously exposed by US media outlets that have revealed how data brokers provide sensitive information to law enforcement and federal agencies (Sarkesian, 2021, Sobel, 2024), or how they trade information that exposes individual mental health conditions (Kim, 2023). The only exception is that a small handful of states have passed legislation targeting the data broker industry; the most notable is California's DELETE Act, which creates a data broker registry and a universal deletion mechanism (California Privacy Protection Agency, 2023). In conclusion, the evolution of the data broker industry highlights the critical need for robust regulatory frameworks that address the complexities of body-focused data collection. **While the EU's regulatory framework is better suited to protect users from the industry, significant challenges persist regarding existing permissions** and the general public's understanding of the data economy. Conversely, the US faces a substantial regulatory gap, with limited federal oversight allowing data brokers to operate with minimal restrictions. Despite initiatives like California's DELETE Act, existing legislative efforts have proven insufficient to fully mitigate the risks associated with the commercialization of sensitive bodily data.

Table: Key harms associated with body-focused data collection

Cybersecurity breaches: Significant rise in cybersecurity breaches affecting bodily and health data.	5,887 large healthcare data breaches reported in the U.S. between 2009 and 2023, escalating from 18 incidents in 2009 to 745 in 2023.	HIPAA, 2024
	MyFitnessPal data breach compromising sensitive information of approximately 150 million users.	Masuch et al, 2021, Aswathi et al, 2022
	215 healthcare-focused cybersecurity incidents reported in the EU from 2021 to 2023.	ENISA, 2023
	Massive cyber attack in Ireland paralyzing healthcare institutions nationwide.	Perlroth and Satariano, 2021
	An unsecured database revealing over 61 million health-related records from Fitbit and Apple HealthKit accessible to the public.	Fowler, 2021
	Change Healthcare facing a ransomware attack by the ALPHV group, resulting in the potential sale of over 4 terabytes of stolen data on the dark web, following a $22 million ransom.	Vicens, 2024
	Compromised health data frequently sold and resold on the dark web, leading to elevated risks of identity theft and exploitation.	Patterson and Kates, 2019

Data misuse and consent violations: Growing exploitation of sensitive bodily data through unauthorized sharing and trading.	Data brokers selling information identifying individuals based on mental health diagnoses, such as depression and anxiety, without consent.	Kim, 2023
	Fitness trackers leaking users' location data even when users had established privacy zones in app settings.	Dhondt et al, 2022
	Health apps like Talkspace and Crisis Text Line shared sensitive mental health conversations with researchers without explicit consent.	Hill and Krolik, 2020, Hendel, 2022
	23andMe shared users' genetic data with pharmaceutical companies for research without obtaining explicit consent.	Demopoulos, 2024
	Reproductive health apps, like menstrual tracking app Flo, sharing sensitive data without obtaining explicit user consent.	IAPP, 2024
	Biometric firms like Clearview AI sharing unauthorized collections of billions of facial images.	Hart, 2022
	Online gambling platforms targeting people with behavioral characteristics of at-risk gambling.	Guillou-Landreat et al, 2021
Discrimination and bias: Rise in discriminatory and/or ineffective decisions based on flawed, biased and inaccurate AI models, as well as overreliance on emerging technology solutions that lack scientific foundations.	Leaked health data increasing insurance premiums for individuals with pre-existing conditions, such as diabetes.	Allen, 2018
	AI systems misidentifying darker-skinned individuals at rates of up to 34%, leading to wrongful arrests.	Buolamwini and Gebru, 2018
	AI-driven diagnostic tools trained predominantly on lighter-skinned images resulting in lower accuracy for darker-skinned patients.	Wen et al, 2022
	AI-powered recruitment algorithms discriminating against individuals with disabilities by relying on criteria that do not accurately measure their job-related skills, such as optimism or emotional stability.	Center for Democracy and Technology, 2020, Access Now, 2023
Persecution, surveillance and other life-threatening impacts: Increase in biometric persecution, exclusion from basic services, and hazardous recommendations from AI models.	American donors in Afghanistan leaving behind biometric data after withdrawing from the country, putting locals working closely with US agencies in considerable danger after the Taliban takeover.	Guo and Nori, 2021
	The UNHCR collecting biometric information from Rohingya refugees and sharing with the Bangladeshi government, jeopardizing the safety and security of a persecuted population.	Human Rights Watch, 2021
	Biometric systems like Aadhaar in India preventing vulnerable individuals and families from accessing essential resources, including food.	The Wire Staff, 2018
	AI-powered chatbots suggesting suicide to users in crisis moments.	Xiang, 2023



CHAPTER 2

Public attitudes around bodily data collection

In this next chapter, we explore the intricate landscape of public opinion on bodily data collection, emphasizing how diverse interpretations and contexts influence public narratives. This investigation seeks to deepen the understanding of public sentiment and the specific factors that influence how people view different forms of data sharing, particularly in contexts like scientific research, law enforcement or commercial gain. Exploring this dynamic is essential, as public sentiment significantly shapes legal and policy frameworks for data protection. Our analysis will highlight potential discrepancies between industry narratives and consumer concerns, particularly regarding privacy and the desire for more control over sensitive data.

2.1. Existing research

Existing literature reveals that **there is a broader recognition of the benefits of body-focused data collection, however, concerns about privacy and security are significant and ever growing**. Public attitudes are heavily influenced by demographic factors like age, education, or gender, and previous experiences with such data collection practices (Perrin et al, 2021, Kalckreuth et al, 2023, Purdon, 2023). Peer influence, family attitudes, education levels and technical know-how also play an important role (Perrin et al, 2021, Aljedaani et al, 2022 Kalckreuth et al, 2023, Alhammad et al, 2024). Attitudes toward data collection are highly context-dependent, showing significant differences across and within domains like commerce, law enforcement and healthcare (Ioannou et al, 2020, Moriuchi, 2021, Skalkos et al, 2021, Pew Research Center, 2021). This indicates that the **public's understanding and acceptance of bodily data collection is not static**; for instance, Moriuchi (2021) found that consumers generally exhibit stronger trust in biometric payment systems during in-store transactions compared to online purchases, illustrating how contextual elements can drastically alter individuals' comfort levels with the same data collection practices. Furthermore, research from the Ada Lovelace Institute (2019) and Ritchie et al (2021) both found that people exhibit a greater, albeit conditional, trust in the public sector's use of

biometric data collection, while demonstrating significant distrust toward advertisers, technology companies, and retailers (Ada Lovelace Institute, 2019, Ritchie et al, 2021).

Relatedly, the phenomenon known as the **"privacy paradox"** frequently emerges in the literature, emphasizing that individuals may acknowledge potential privacy risks yet remain inclined to share personal information in exchange for tangible advantages (Ioannou et al, 2020, Zhang et al, 2021, Purdon, 2023). This paradox reflects the complex interplay between individuals' concerns for their privacy and their desires to access services or benefits that require such data sharing. Moreover, there is a resounding demand among the general public for increased transparency regarding data handling practices; with people expressing a strong need for clear communication about how their data will be utilized, shared, and safeguarded (Perrin et al, 2021, Kalckreuth et al, 2023, Purdon, 2023).

2.2. Our survey findings

In order to deepen understanding of public sentiment toward body-focused data collection, we conducted two public surveys aimed at exploring attitudes and perceptions around such data practices. The goal was to **extend existing research on the "privacy paradox" by analyzing its manifestation across diverse contexts**, through examining how contextual factors—such as the specific purposes for data sharing, including research versus commercial gain—impact public acceptance. While prior work acknowledges the tendency of individuals to share personal data despite acknowledging risks, we aimed to investigate the specific interplays between privacy concerns and perceived utility, through comparing the various trade-offs that people make between privacy and benefits in different situations.

Our study also aimed to expand on previous research that primarily highlights the public's demand for transparency by directly examining how information disclosure affects attitudes toward data sharing. Existing literature often neglects the emotional and psychological impacts of data collection on individuals, especially in sensitive contexts involving unauthorized access or data misuse. To address this, our research employed a scenario-based approach to **elicit emotional responses related to specific situations of data misuse**, capturing another layer of the complexities of public sentiment surrounding body-focused data collection. Additionally, existing literature frequently overlooks the broader societal implications of bodily data collection as a whole, failing to recognize the interconnectedness of various data types and their cumulative effects on public trust and engagement.

To address some of these gaps, our first survey focused on examining respondents' engagement with electronic health records, mobile health apps, and biometric technologies. It **assessed their willingness to opt out of these systems based on various conditions, their perceptions of data access control, and their comfort level with sharing data for scientific research versus financial gain**. The second survey employed a scenario-based approach to specific situations involving data misuse, such as unauthorized sharing of health information or biometric data. By analyzing both qualitative and quantitative responses, we aimed to capture the complexities of public sentiment surrounding body-focused data collection, including the factors driving trust and concerns among users.

◇ **The findings revealed that a substantial majority of respondents engaged with some form of bodily data collection,** primarily through electronic health records (80.2%), mobile health apps (76.2%), and biometric techniques (73.6%). Key avenues included mandatory health record systems; fitness, exercise

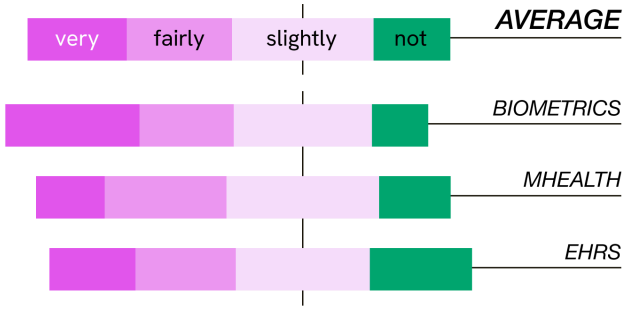
and nutrition apps; mental health and meditation as well as fingerprint, facial and voice recognition in the biometric context. The demographic composition of the participants showed a balanced mix of genders across all age ranges, with the majority coming from younger generations (ages 18-24 and 25-34). Most respondents held at least a bachelor's degree, and many had master's or doctorate degrees, reflecting higher levels of education.

◇ **The survey results reveal varying levels of concern among respondents regarding unauthorized access to their health data across different areas.** About 44% expressed significant worry about Electronic Health Records (EHRs) being accessed by individuals other than their treating doctors, while approximately 31% were slightly concerned, and 24% were not concerned at all. In the context of Mobile Health Apps (mHealth), nearly 47% voiced strong concerns about unauthorized access beyond app developers and service providers, with around 36% feeling slightly concerned and 17% feeling concern. These trends emphasize a strong worry about biometric data privacy, with respondents generally feeling less concerned about the security of EHR systems.

◇ **With regards to access control, the survey results indicate that individuals exhibit confidence in understanding who has access to their health data, yet there is less assurance about the restrictions on that access.** For EHRs, 47.50% of respondents believed that only those who treat them or provide direct services have access to their health data, while 41.10% suspected that secure. The highest level of concern was noted for biometric techniques, where over half of respondents (54%) expressed serious apprehension about access by others outside the collecting organizations, while about 33% remained slightly concerned and 13% reported no others, including medical professionals who do not treat them and third parties, might also have access; 11.40% were unsure. In the mobile health context, a

HOW CONCERNED ARE YOU?

How concerned are you that besides the service providers, others may have access to your bodily data?

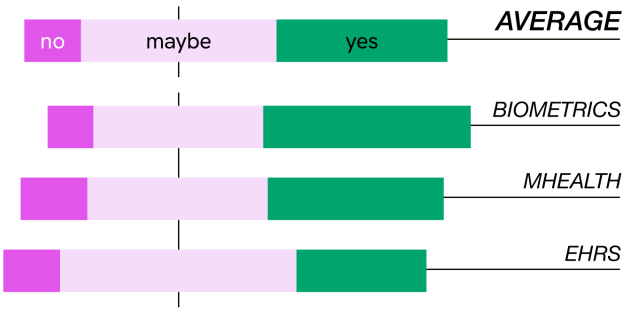


smaller percentage (36.60%) felt that only their direct service providers had access to the data they shared, with 32.20% believing that others could access it, and 31.20% uncertain. Regarding biometric data, a higher confidence was noted, with 52.50% stating that only those treating them have access, while 21.80% thought others could access this data, and 25.70% were unsure. Overall, these patterns reveal a trend where individuals feel they know who can access their data yet remain apprehensive about whether access is truly restricted.

◇ **A considerable number of respondents expressed a willingness to opt out of data collection practices when there are concerns about unauthorized sharing.** For Electronic Health Records (EHRs), 30.70% of respondents would opt out if their data was shared beyond their treating physicians, while 55.90% were uncertain, and 13.40% would not opt out. In the case

OPTING OUT

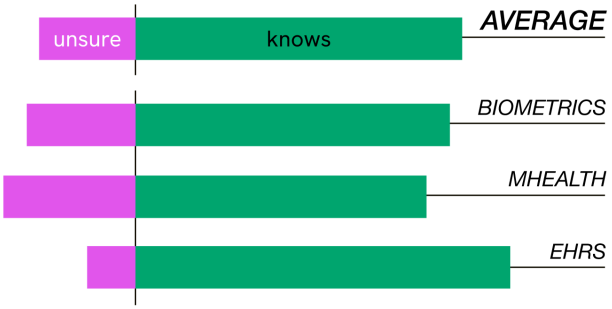
Would you consider opting out of these systems if you learned that your bodily data was shared beyond your service providers?



of Mobile Health Apps (mHealth), 41.60% said they would opt out under similar circumstances, with 42.60% unsure, and 15.80% indicating they would not. When it comes to biometric data collection, 49% were willing to opt out if their information was shared, 40.10% were uncertain, and only 10.90% would not opt out. These patterns highlight that a considerable number of individuals express a willingness to opt out of data collection practices when there are concerns about unauthorized sharing, underscoring prevalent privacy anxieties.

UNDERSTANDING ACCESS CONTROL

Who do you think has access to your bodily data?



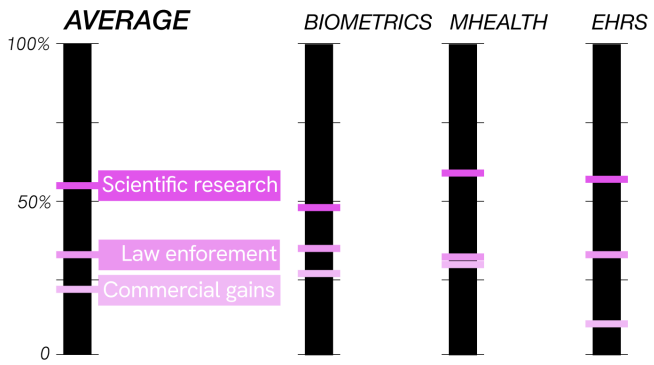
◇ **Survey participants expressed varying levels of confidence in their ability to opt out of data collection methods.** Regarding electronic health records (EHRs), nearly half (47%) felt they could not stop using these systems, while 26.2% believed they could opt out whenever they chose, and about 24.3% were unsure. In contrast, a more positive outlook emerged for mobile health apps, with 56.4% feeling they could stop using these apps at will; however, 24.3% noted that their ability to opt out depended on specific situations, and 12.9% felt they could not opt out at all. Opinions on biometric data collection were split as well, with 33.7% believing they could opt out mechanisms and improved transparency from data collectors.

◇ **Survey respondents conditionally accepted data sharing, prioritizing transparency and purpose.** A significant majority indicated they were comfortable with their bodily data being used for health benefits, particularly in scientific research, which yielded high acceptance rates of 57.4% for electronic health records (EHRs) and 59.4% for mobile health apps. However, acceptance significantly declined when it came to profit-driven purposes, with only 10.9% supporting such uses of electronic health records (EHRs), compared to 29.7% for mobile health apps, and 26.7% for biometric data. Responses regarding access by law enforcement were also mixed; while acceptance rates were lower, they were still notable, ranging from 32.7% for EHRs to 35.1% for biometric data. On average, acceptance for sharing data for scientific research was 54.77%, while support for law enforcement access stood at 33.17%, and significantly less at 22.43% for commercial gains. This data highlights the nuanced attitudes of respondents toward data sharing, suggesting a willingness to participate in data exchange when personal health benefits and clear purposes are evident, but also a discernible wariness concerning profit-oriented and law enforcement uses.

◇ **With regards to app-specific concerns, participants showed a strong awareness of the various privacy risks tied to different app categories.** Regarding electronic health records, participants expressed significant concern about data sharing beyond their treating physicians, particularly when done without informed consent. For mobile health app data, concerns were highest for sensitive data types (mental health, reproductive health) and for profit-driven sharing without compensation. App users showed a greater willingness to accept data sharing for research, but a strong desire for transparency and opt-out options persisted. Women's health apps sparked significant concerns, reflecting the sensitivity of the data involved. Similarly, mental health and substance abuse apps created a strong negative reaction regarding data sharing, underscoring the need for enhanced privacy

SHARING PREFERENCES

I don't mind if my bodily data is shared further if it's for...
(multiple options were possible)



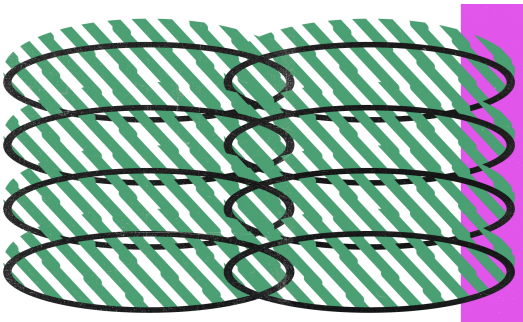
Source: "Skin to Screen" research paper, Julia Keseru 2024

protections in these areas. Biometric data generated the strongest negative reactions, especially concerning facial recognition and iris scans. Facial recognition data elicited particularly strong negative responses, likely due to its potential for surveillance and misuse. Fingerprint and iris scans also raised notable apprehension, highlighting the broader unease associated with biometric data.

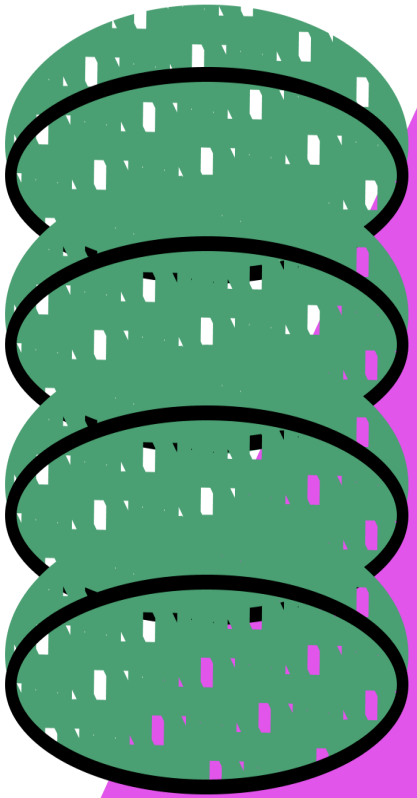
◇ **Responses revealed overwhelmingly negative sentiments towards the sharing and sale of bodily data, particularly when done without explicit consent and transparency.** Participants consistently expressed outrage and a sense of exploitation in scenarios where their health data was sold for profit without their knowledge or any financial benefit to them. The use of biometric data (facial recognition, fingerprints, iris scans) was viewed with extreme suspicion. Positive or neutral responses were largely confined to scenarios offering direct personal benefit (e.g., personalized fitness recommendations, new treatments for their specific condition) or the potential for profit sharing. Even in these scenarios, the desire for transparency and prior notification remained strong.

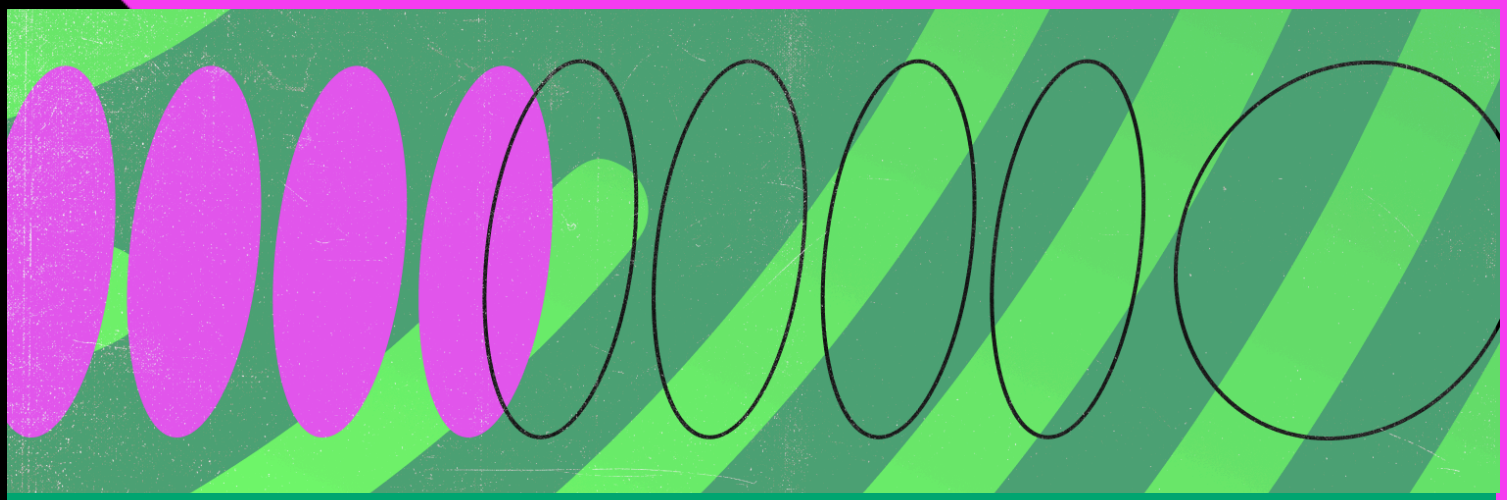
◇ **With regards to public sentiment, the most common terms associated with non-consensual data sharing scenarios were highly negative.** In the context of cyber extortions, common terms included "anger," "fear," and "distrust." Similarly, phrases like "invasion of privacy," "unacceptable," and "dangerous" were frequently used in the context of leaked health data and its impact on insurance costs. Regarding fitness trackers sharing data with third-party firms, 54.5% of respondents expressed significant concern, citing feelings of "betrayal," "manipulation," and "exploitation." In scenarios where mental health data was shared for research without consent, 53.1% of participants described their concerns with terms like "untrustworthy," "invasive," and "manipulative." Concerns about law enforcement access to health records were also significant, with 38.4% expressing high levels of anxiety, using words such as "anger," "fear," and "insecurity." The consistent appearance of phrases like "without my knowledge," "without my consent," and "I should have control" underscores the paramount importance of transparency and informed consent in data handling practices.

◇ **Across all three domains, a consistent pattern emerged: the optimism conveyed by the technology industry often stands in stark contrast to public sentiment regarding the associated risks and harms.** Specifically, survey responses highlight a significant gap between industry promises and user perceptions, suggesting that while individuals may recognize the potential benefits of body-focused data technologies, and even rely on these systems for their own comfort, they remain deeply concerned about issues such as unauthorized data sharing, misidentification, discrimination and overall data management issues. This indicates that public apprehensions are not just theoretical but grounded in a desire for clarity and accountability.



To conclude, our survey findings illustrate a **clear unease among individuals about contemporary data sharing practices surrounding bodily data**, with significant numbers expressing concerns over unauthorized access and inadequate protections. Our findings highlight a profound disconnect between the advancements in technology and the public's expectations for privacy and data security; while the frustration and anxiety voiced by respondents emphasize an **unanimous desire for stronger protections and clearer regulations governing the collection and use of bodily data**. Emotional reactions to scenarios of data misuse frequently included feelings of betrayal, manipulation, and invasion of privacy, emphasizing the psychological impact of such violations. Such public concerns should serve as a catalyst for re-evaluating and redefining the legal interpretations and protections currently governing body-focused data practices.





CHAPTER 3

A rights-based approach to bodily data collection

While body-focused technologies promise significant benefits in health and well-being, they also present considerable challenges, as outlined in Chapter 1. Additionally, Chapter 2 highlighted a significant disconnect between the desired standards of data privacy and prevailing industry practices, revealing public concern over how bodily data is managed. Current legal frameworks, primarily centered on data protection, fail to address these challenges, neglecting the broader implications of bodily data harms on fundamental rights such as integrity, dignity, and personal agency. This necessitates a shift from data-protection-centric approaches to a broader rights-focused framework that acknowledges the complex interplay between emerging digital technologies and human rights.

In response to these challenges, our research advocates applying existing human rights frameworks, particularly the right to bodily integrity, to address emerging data issues by introducing the concept of "databody integrity." This framework aims to align more closely with autonomy, integrity, and dignity in the digital context, and includes calls for strategic litigation to reinforce bodily integrity and push for updated laws and policies addressing digital threats. Introducing the concept of databody integrity also aims to address the discord between industry practices, legal trends, and public opinion, fostering a sense of autonomy in an environment where data collection often occurs without informed consent. Additionally, we propose a detailed taxonomy of databody integrity violations to more clearly identify frequently compromised rights and values.

3.1. The right to bodily integrity

Bodily integrity is a cornerstone of contemporary human rights frameworks and has garnered significant attention in legal and political debates throughout the 20th century (Viens et al, 2013, Herring and Wall, 2017, Townsend, 2023, Patella-Ray, 2017). While it is not a standalone human right, **safeguarding against violations of the body is fundamental to various human rights**

instruments, such as the freedom from torture, slavery, arbitrary detention, or the right to privacy (Viens et al, 2013, Herring and Wall, 2017, Townsend, 2023). Many constitutions around the world incorporate some form of protection for bodily integrity, reinforcing the essential role of bodily integrity in upholding human dignity and security. Unlike bodily autonomy, bodily integrity encompasses *both* the freedom to make autonomous choices *and* the right to be free from unwanted interference (Ibid).

The concept of bodily integrity has evolved significantly in the 20th century, especially since World War II. After the rights violations and medical experiments of the Nazi regime were exposed to the world (Annas and Grodin, 1999, Frewer, 2010, Gallin and Bedzow, 2020), the Nuremberg Trials played a key role in shaping modern discourse around human rights in general, and around the right to integrity and dignity in particular. The trials eventually resulted in the establishment of the Nuremberg Code, a set of principles that have been guiding the moral and legal discourse around research practices ever since (Annas and Grodin, 1999, Frewer, 2010), mandating the "voluntary consent of the human subject" in any human experimentation. The trials also paved the way for the Universal Declaration of Human Rights (1948), a landmark document that promotes bodily integrity both through its protections (around the right to life and security, for instance), and its prohibitions (against torture and degrading treatment, amongst others) (Dicke, 2001, Viens et al, 2013, Addis, 2019).

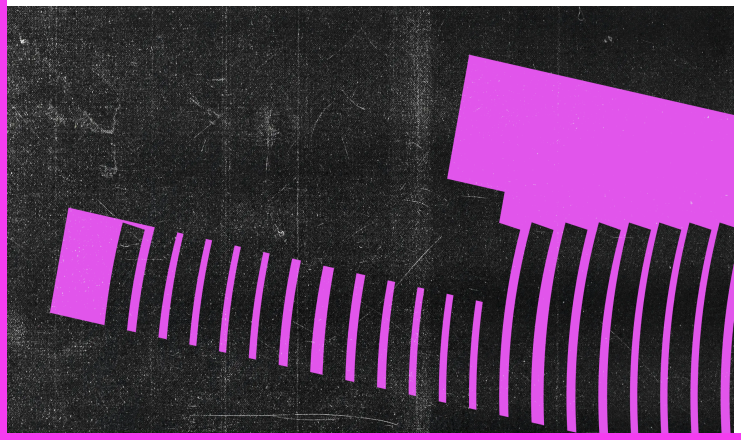
In addition to these foundational documents, the International Covenant on Civil and Political Rights (ICCPR1967) includes implicit safeguards for bodily integrity, protecting **against unlawful harm and non-consensual medical experimentation**. Ethical frameworks like the Declaration of Helsinki (1964) or the Belmont Report (1974) also significantly enhance the protection of bodily integrity, particularly in medical and clinical research settings. These legal instruments underscore the importance of respecting autonomy in healthcare decisions, establishing the right to integrity and dignity as fundamental principles of medical law (Herring and Wall, 2017, Gronowski et al, 2019, O'Sullivan et al, 2020, Nagai et al, 2022). Consequently, these documents necessitate that healthcare providers inform patients about the nature, risks, and benefits of treatments, ensuring that consent is informed and voluntary. Meanwhile, the Convention on the Elimination of All Forms of Discrimination Against Women (1979) recognizes **reproductive rights as essential to bodily integrity.**

More recently, the **Charter of Fundamental Rights of the European Union has emerged as a crucial legal document for the right to bodily integrity,** explicitly articulating individuals' rights to both physical and mental well-being in Article 3 (European Union Agency for Fundamental Rights, 2009). This charter is significant in establishing and safeguarding bodily integrity as a fundamental right within the context of European law (European Union Agency for Fundamental Rights, 2009), for several reasons. Within the domains of medicine and biology, the document emphasizes the importance of free and informed consent, while forbidding the act of making the human body and its parts "a source of financial gain". The Charter also addresses inhumane treatment and degradation in Article 4, the respect for private life in Article 7, the protection of personal data in Article 8, and several other fundamental rights that, as described above, are frequently violated through intrusive data collection practices (Ibid). In the US, bodily integrity is primarily protected by the Constitution's Fourteenth Amendment and its Due Process Clause, including rights like the freedom to refuse unwanted medical procedures (Baxter, 2024, US Congress, 2024). The Fourteenth Amendment is often interpreted by the Supreme autonomous bodily decisions, as we will describe below.

Despite its significance in "offline" contexts, **bodily integrity is largely overlooked in digital contexts**. Notable exceptions include the work of PJ Patella-Ray, who argues that the bodily integrity framework more accurately captures the violation felt by victims of non-consensual pornography compared to existing privacy regimes (Patella-Ray, 2017). Similarly, research by Anja Kovacs and Tripti Jain highlights how non-consensual data sharing impacts autonomy, dignity, and bodily integrity (Kovacs and Jain, 2021). Additionally, Vardanyan et al. argue that the concept of digital integrity provides a more effective framework for addressing online human rights violations than current data protection regimes (Vardanyan et al, 2022).

3.2. Bodily integrity in the courts

Case law plays a crucial role in the interpretation of fundamental rights, including the right to bodily integrity. Judicial decisions can clarify legal ambiguities, create clear precedence and help adapt decades-old documents for new socio-political contexts (Resnik, 1987, Dworkin, 1988, Bassiouni, 2013, Donelly and Whelan, 2020). Judicial rulings also play an important role when a right is not absolute as it may violate other people's rights or the public interest. In the context of bodily integrity, this has been especially striking during the Covid pandemic when quarantine restrictions and mandatory vaccinations were often seen as infringing on people's individual right to bodily integrity (Ignovska, 2023, Alekseenko, 2022).



Pertinent case law around bodily integrity encompasses a variety of judicial rulings around reproductive rights, genital mutilations, non-consensual medical treatments, organ transplants, euthanasia, and increasingly, the regulation of medical devices and implants (Viens et al, 2013). A striking example for ambiguous interpretations is the **domain of reproductive rights, where bodily integrity has been interpreted in highly contradictory ways** –both in favor of abortion as an avenue to protect women's autonomous bodily decisions, and against pregnancy termination as a way to assert the rights of the fetus (Paltrow et al, 2022, Petersen, 2023, Nwano et al, 2024).

Roe v. Wade, the highly contested (and since overturned) US Supreme Court ruling has been pivotal in the context of bodily integrity, establishing **strong protections around autonomous decisions regarding a woman's body** (Ibid). Still within the domain of reproductive rights, the case of St George's NHS Trust v S. stands out, where an emergency cesarean section was performed on a woman against her wishes, where the judge ruled that no one should be "forced to submit to an invasion of her body", regardless of the consequences (Marshall, 2013).

The sharing and trade of biological data like blood and DNA samples, or human organs, have regularly come up at courts in the context of bodily integrity. In the case of S. and Marper v. In The United Kingdom, the European Court of Human Rights (ECHR) ruled that the blanket retention of DNA samples and fingerprints violate the right to respect for private life, even in the context of law enforcement (European Court of Human Rights, 2008). Moore v. Regents of the University of California was

another important case that addressed the commodification of biological data. Moore filed the lawsuit because his blood and tissue samples were used without his knowledge by the University of California, for both financial and scientific purposes. And although the US Supreme Court eventually ruled against him; the judges concluded that the university should have informed Moore of how they intended to use his biological data (JUSTIA US Law, 1990).

Overall, these judicial rulings have shaped the legal landscape by clarifying ambiguities and establishing precedents that safeguard individual rights to integrity and autonomy, while also addressing broader societal needs. In the next section, we will analyze how these rulings regarding the right to bodily integrity can be interpreted within the digital context, particularly in light of the potential harms we have examined earlier.

3.3. The right to "databody integrity"

To be able to provide concrete recommendations on how bodily integrity can mitigate the increasing harms associated with bodily data collection, we now introduce the concept of **"databody integrity."** This framework will enable us to identify critical areas for strengthening individual rights and inform our strategic recommendations for safeguarding autonomy and dignity in the face of emerging digital threats. This term **refers to the inviolability of individuals' online personas and their right to control the handling of data that reflects their unique physiological and psychological characteristics.** This definition is rooted in established human rights principles, as previously outlined.

Building on this foundation, we also propose a taxonomy that clarifies the relationship between data governance and bodily integrity. This taxonomy identifies four critical categories of bodily integrity breaches that are relevant in online environments, drawing from legal definitions and principles established in pertinent legal documents and case law. It elucidates how various forms of data misuse can specifically undermine bodily integrity. Implementing this taxonomy can occur through multiple avenues, including strategic litigation, advocacy for new laws and policies, and initiatives to raise public awareness about online privacy. The identified categories are as follows:

◇ **Non-consensual scientific experimentation is defined as the use of bodily data for research purposes without informed user consent.** This category may refer to practices where people's bodily data, including their health records, biometric data, or behavioral characteristics, is used for scientific purposes without clear permission. This category is grounded in various existing international laws and regulations, including the ICCPR, the Charter of Fundamental Rights of the EU, the Declaration of Helsinki, and the Belmont Report, all of which emphasize the necessity of obtaining informed consent and ensuring ethical treatment of individuals in research, as described above. Previously mentioned examples include the cases of Talkspace and Crisis Text Line who shared sensitive mental health with third party researchers, creating significant public outcry about the ways in which the mobile health industry is exploiting people in crisis situations (NYTimes, 2020, Politico, 2022).

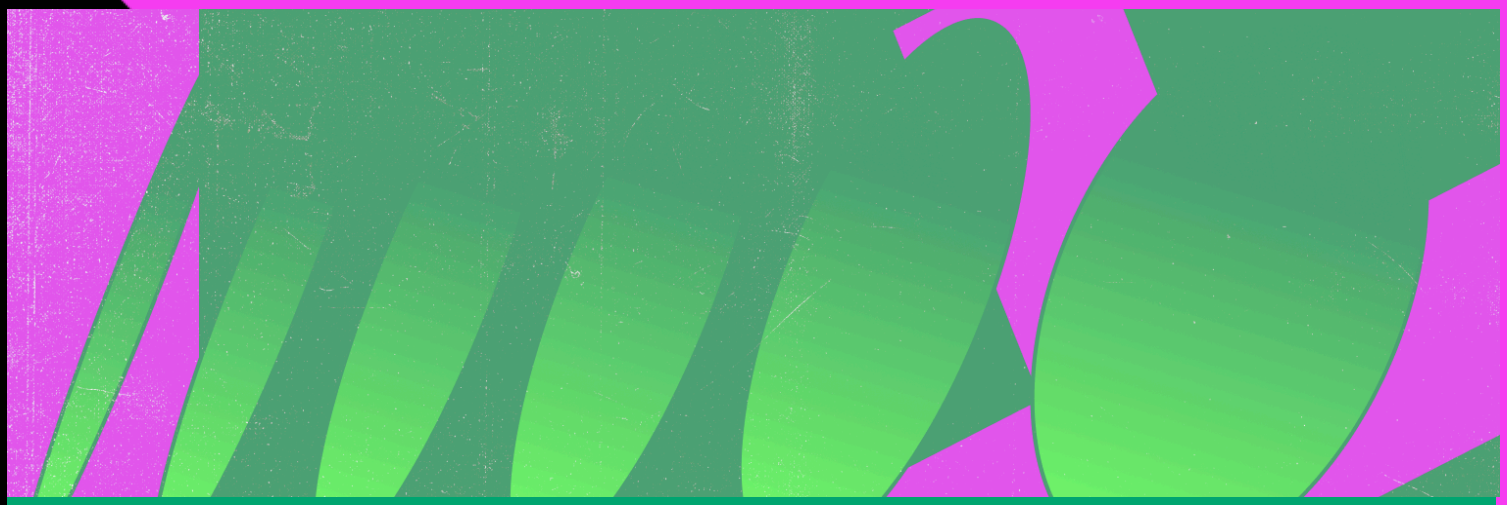
◇ **Non-consensual financial gains refer to the monetization of bodily data without meaningful user consent.** This category is grounded in data protection regimes like the GDPR, which mandates explicit consent when sensitive data is processed for the financial gain of the data handler, or the Charter of Fundamental Rights of the European Union that explicitly prohibits the commercialization of the

human body and its parts as a source of financial gain. A prominent example of this breach is the data-broker industry's practice of collecting extensive amounts of bodily data from diverse sources and selling that information to advertisers and other interested parties, as described in Chapter 1 (Keagen and Eastwood, 2023, Kanwal and Walby, 2024, Morrison, 2020, Armitage et al, 2023). Trading with user health data is another notable example, as seen with the menstrual tracking app Flo who shared intimate details about period cycles and sex life with companies like Facebook (Clayton et al, 2022). The emerging practice of genetic testing companies, like 23andMe, to share aggregated genetic data with pharmaceutical companies can also be seen as notable examples of such rights violations (Demopoulos, 2024).

◇ **Non-consensual bodily modifications** can refer to the unauthorized collection, use, and manipulation of people's biometric or health data in ways that can affect their health status or bodily characteristics without explicit approval. Such a category can be supported by the Convention on the Elimination of All Forms of Discrimination against Women, as well as the various human rights documents described above that prohibit inhuman or degrading treatment. In the online context, this might include targeted advertising based on data gathered from wearable devices that encourage users to modify their behaviors according to commercial interests rather than personal choice (Sui et al, 2023). For example, users who wear fitness trackers may receive personalized ads for weight loss products based on their exercise regimes, products that directly impact their bodily choices. Targeting based on mental health data can influence individuals' mental states and health decisions, shaping behaviors without their knowledge (Callanan et al, 2021, Rossmaier, 2022).

◇ **Violations of psychological integrity can arise from various forms of data misuse,** causing severe psychological harm that contravene human rights frameworks that prohibit inhuman or degrading treatment.The exposure of health, mental health, or reproductive information, for instance, can lead to unwanted scrutiny and stigmatization, as well as wide-spread bullying and discrimination (Patella-Ray, 2017, Sobieraj, 2020, Citron, 2023, Shires et al, 2024). The exploitation of biometric data is another noteworthy example, as it creates a profound sense of fear and vulnerability among individuals who may be subjected to harm or persecution, as witnessed with Rohingya refugees from Myanmar (Human Rights Watch, 2021). It's important to note here that the of Human Rights (ECtHR) has emphasized that the definitions and thresholds for degrading treatment are not static but can evolve with societal progress, mandating that legal interpretations adapt in response to shifting societal values around psychological harm (Arai-Yokoi, 2003).

While the establishment of new laws and policies can support the integration of such concepts into diverse contexts and under emerging threats, **the proposed taxonomy provides the opportunity to advocate for this fundamental right within the framework of existing rights and laws**. This approach not only reinforces existing human rights principles (Ligthart, 2024) but also sets a precedent for holding technology companies accountable, even in absence of new legislation. It's important to note here that many of the harms associated with body-focused data collection may infringe on other fundamental rights as well, not only bodily integrity. This includes the freedom of thought, freedom of assembly and association, the right to respect for private and family life, or the right to be free from discrimination. And while it falls outside the scope of our research, we strongly encourage experimenting with a similar analytical approach in the context of other fundamental rights. The combination of these efforts can ultimately provide a more comprehensive understanding of the connections between data misuse and human rights.



CHAPTER 4

Recommendations

The recognition of databody integrity as a critical framework underscores the need to align legal protections with the evolving realities of technological advancements. This perspective suggests that incorporating a rights-based framework is not only a response to the public's demand for greater transparency and accountability but also a fundamental requirement for safeguarding human rights in a rapidly digitizing world.

This emphasis on databody integrity is crucial, as many emerging risks associated with bodily data collection—such as unauthorized sharing, algorithmic bias, and excessive surveillance—are inadequately addressed by traditional data protection frameworks. Current regulations often prioritize data safeguarding over the holistic protection of individuals' rights, failing to consider the nuanced impacts of technology on personal identity, dignity, autonomy and integrity. To effectively address the concerns raised in Chapter 2, the evolution of legal frameworks surrounding body-focused data collection must integrate principles of bodily integrity and user consent. The inadequacies highlighted in existing laws emphasize the urgent need for updates and reforms that reflect contemporary practices and the public's expectations for privacy protection. Together, these insights highlight the pressing need for **improved transparency, meaningful consent mechanisms, user control, and comprehensive legal protections to effectively address public concerns and safeguard the integrity of individuals' bodily data in an increasingly complex digital landscape**. In this next chapter, we will therefore provide targeted recommendations for policymakers, activists, and technology industry representatives based on the research findings.

4.1. Recommendations for policymakers

◇ **Incorporate the concept of "databody integrity" into existing legislation:** Explicitly define and incorporate the concept of "databody integrity" into existing data protection, online privacy and emerging technology legislation. Reinforce legal protections targeting non-consensual bodily data collection and

establish clear guidelines on how personal bodily data should be processed. Legislation concerning behavioral targeting, predictive analytics, recommendation algorithms, and content moderation, could also encompass the concept of "databody integrity" to mitigate manipulation based on innermost feelings and thoughts. Furthermore, addressing databody intrusions that feel like physical violations—such as online gender-based violence, image based abuse, or Extended Reality (XR) harassments—might also benefit from a more robust recognition of the intersection of physical and digital bodily rights.

◇ **Broaden the definitions of what constitutes sensitive or special category data:** Expand current definitions within data protection regimes and technology regulation to include specific categories of sensitive data, particularly encompassing all forms of bodily data collection, which should be classified as sensitive or special category data requiring heightened protections. This expanded definition should explicitly include "derived data" or "inference data," clarifying that information derived from analysis or aggregation—such as biometric measurements, health trends inferred from wearable devices, and even location data linked to health behaviors—can pose significant privacy risks. For instance, regulations could mandate safeguards like advanced encryption for stored bodily data and explicit user consent for the use of inferred data, as well as establish strict guidelines on data retention and sharing practices. Furthermore, regulations should require regular audits to assess compliance with these definitions, ensuring organizations maintain transparency in their data usage practices and individuals have insight into how their data might be aggregated or inferred, thereby reinforcing privacy protections in a rapidly evolving technological landscape.

◇ **Strengthen enforcement around meaningful consent mechanisms:** Enforce robust provisions for informed consent, ensuring explicit user consent is obtained for each specific use of sensitive bodily data. Mandate that data controllers clearly communicate how the data they collect will be used, potential risks, and who will access it, to prevent ambiguous or generalized consent practices that could lead to unauthorized data exploitation. Mandate standardized and user-centric consent forms across jurisdictions to enhance consistency and transparency in the consent process surrounding bodily data collection. These forms should be easy to understand and user-friendly, offering clear and accessible information about data collection practices.

This approach minimizes disparities between different regulatory environments, helping individuals make informed decisions and fostering trust in data protection practices.

◇ **Broaden scope and applicability of existing technology regulation and data protection frameworks to more effectively regulate emerging technologies:** This involves modifying frameworks to encompass protections for contemporary data contexts, such as mobile health applications and biometric data technologies, extending safeguards beyond traditional settings. Regulations should be applicable across various environments—healthcare, law enforcement, consumer technology—by focusing on the nature and impact of the data rather than the setting it is collected in, ensuring adaptability and resilience in new contexts. Specifically, HIPAA in the US could be modified to cover mobile health apps and biometric data, thereby expanding protections beyond conventional healthcare. Consider including organizations that are neither covered entities nor business associates, thereby regulating any platform where health-related information is exchanged. However, this would require redefining

healthcare within HIPAA, likely imposing stringent compliance requirements on many organizations (Clayton et al, 2023).

◇ **Strengthen cybersecurity standards and offer more proactive support to organizations collecting body-focused data:** Implement rigorous security and interoperability protocols to ensure data protection across various systems and sectors, mitigating the risk of unauthorized access and breaches. Aligning these standards internationally will promote a unified defense against the rise of cybersecurity threats that are global in nature.

Recognize that not all organizations possess the necessary expertise or resources to comply with strict regulations. Offer support through accessible training programs, technical support, and resource-sharing platforms that help organizations build their capability to meet these requirements effectively, especially in a fast-changing technical environment.

◇ **Invest in encryption and cybersecurity standards, tools, and applications to enhance data security:** Relatedly, allocate resources to develop and implement robust encryption technologies that protect sensitive information against unauthorized access and cyber threats. Establish standardized cybersecurity protocols tailored specifically for organizations that handle body-focused data, ensuring comprehensive measures for data protection and privacy. Promote investment in advanced cybersecurity tools and applications that facilitate real-time monitoring and threat detection, enabling organizations to respond proactively to potential security breaches. Foster collaboration among industry stakeholders to share best practices and innovative solutions, thereby building a more resilient cybersecurity ecosystem.

◇ **Tighten regulations on data brokers:** Establish a universal data broker registry requiring full disclosure of data sources and types, empowering consumers with opt-out and data deletion mechanisms. Provide consumers with robust access and control over their data profiles, including correction and usage limitation options. Standardize reporting requirements for the industry to ensure clarity in how data is collected, used, and shared. Introduce certification systems and regular audits to verify compliance and encourage best practices. Increase enforcement measures and penalties for data brokers failing to comply with data protection standards, drawing parallels with rigorous privacy frameworks to ensure adherence and accountability.

◇ **Harmonize global data protection standards:** Craft comprehensive data protection agreements between regions, focusing on databody integrity and facilitating compliance across borders. Develop cross-border data flow protocols to ensure data protection standards are consistently met, and work towards aligning existing national regulations on key aspects such as consent, data rights, and breach notification. Establish detailed protocols specifically aimed at governing the secure flow of data across international borders. These protocols should address the technical, legal, and operational standards required to protect data integrity during transfer, including encryption standards, data handling procedures, and requirements for transparency and accountability.

◇ **Mandate impact assessments for emerging technology solutions:** Require all new data technologies to undergo comprehensive impact assessments, focusing on databody integrity. These assessments should highlight bodily data-related risks, enhancing existing privacy safeguards within data protection frameworks. Require companies to conduct databody integrity impact assessments as part of their data handling

policies, similar to data protection impact assessments under the GDPR. Establish independent boards to review and address ethical concerns related to databody integrity violations. These groups should provide guidance and recommendations for responsible data practices as technologies evolve.

◇ **Invest in alternative data governance models:** Prioritize the development and support of alternative data governance models such as data trusts, decentralized autonomous organizations (DAOs), and data cooperatives to effectively address the complex challenges described in this paper. Establish regulatory frameworks that facilitate the creation and operation of these intermediaries, thus fostering a data ecosystem where individual privacy rights are upheld while enabling responsible data sharing practices. For instance, data trusts can serve as intermediaries that allow communities to collectively manage and govern their data, ensuring benefits are returned to data subjects instead of solely to large corporations. This can be achieved by establishing legal frameworks that enable these entities to negotiate data use terms on behalf of individuals, as seen in successful implementations like the Johns Hopkins Medicine Data Trust. Additionally, DAOs can facilitate decentralized decision-making, allowing members to collectively decide how their data is used and shared, promoting a sense of ownership and agency. Moreover, data cooperatives can act as collective bodies that aggregate data from individuals to create a more powerful negotiating position against data collectors, fostering equitable revenue-sharing models (Duncan, 2023).

4.2. Recommendations for activists groups

◇ **Engage in strategic litigation to encourage judicial systems globally to interpret rights concerning digital bodily integrity through the lens of existing case law.** Use the taxonomy of databody integrity breaches to set legal precedents that recognize and enforce digital extensions of bodily rights. Initiate class action lawsuits that address widespread violations of databody integrity, such as non-consensual financial gain or unauthorized biometric modifications, with the aim of ensuring collective redress. Leverage international human rights law to hold multinational corporations accountable for breaches of databody integrity, and to pursue cross-jurisdictional cases. To illustrate: Judicial rulings can emphasize the need for more rigorous cybersecurity measures to guard public health records, mobile health solutions, biometrics techniques, and other avenues of bodily data collection. Courts could require that data processing organizations implement more transparent and robust data protection practices and cybersecurity measures, thereby ensuring that individuals' sensitive bodily data is safe and secure. Courts can affirm that individuals should not be subjected to invasions of their bodily autonomy without their explicit consent, particularly in the realms of digital health and biometrics. Judicial decisions could establish robust frameworks for enforcing meaningful consent, ensuring that individuals fully understand the implications of how their health and biometric data will be collected, used, and shared. Lastly, judicial rulings can also provide guidance on how to ethically navigate the intersection of individual rights and societal needs, fostering trust in both public health initiatives and the responsible use of bodily data.

◇ **Utilize existing human rights frameworks to bolster litigation and advocacy efforts:** Bodily integrity is a crucial tenet of contemporary human rights discourse, which can be leveraged to advance legal interpretations and protections in the digital realm. By invoking instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, advocates can frame violations of digital bodily integrity—such as unauthorized data collection or non-consensual information sharing—as breaches of fundamental human rights. For example, the principles established during the Nuremberg Trials regarding informed consent provide a foundational basis for arguing that any health-related data collection without explicit user consent is a violation of bodily integrity. Additionally, regional documents such as the Charter of Fundamental Rights of the European Union explicitly support the right to physical and mental well-being while emphasizing the necessity of informed consent in medical and data contexts. By pursuing litigation grounded in these established human rights frameworks, advocates can create legal precedents that articulate the necessity for robust protections against digital violations. Moreover, drawing on constitutional protections in the US, such as those enshrined in the Fourteenth Amendment, can strengthen arguments against invasive practices that undermine bodily autonomy. In doing so, litigation and advocacy efforts can harness the existing legal architecture to ensure that the evolving definition of bodily integrity encompasses digital contexts (Digital Freedom Fund, 2024).

◇ **Leverage existing legal tools such as Freedom of Information (FOI) requests and Data Subject Access Requests (DSARs) to gain insights into the body-focused tech industry:** These tools can be instrumental in uncovering how this rapidly evolving market operates, particularly concerning the relationship between private and public entities. In the European Union, DSARs empower individuals to request information about the types of personal data that organizations collect, process, and share, providing transparency and clarity about data handling practices. By utilizing DSARs, individuals and advocacy groups can examine not only the data collected by companies specializing in body-focused technologies, such as wearable devices and health applications, but also the agreements and data-sharing arrangements between these companies and public institutions. Furthermore, FOI requests can be employed to access information held by governmental bodies about partnerships with private sector actors, regulatory compliance, and data usage policies. This combination of tools allows for a comprehensive understanding of how data flows between public and private sectors, ensuring accountability and fostering responsible data management practices.

◇ **Use the proposed taxonomy of databody integrity breaches to raise public awareness about the importance of databody integrity.** This can drive public support for stronger laws protecting individuals' digital rights. Engage with stakeholders civil society organizations to promote the understanding and adoption of databody integrity principles within digital governance frameworks. Utilize the framework to advise governmental and non-governmental organizations on formulating policies that safeguard digital extensions of bodily rights, and to harmonize global human rights laws to include databody integrity. Develop guidelines that technology companies and researchers must follow to ensure compliance with databody integrity standards.

◇ **Establish watchdog groups dedicated to monitoring compliance with databody integrity.** Employ a variety of methodologies, including analyzing public reports, scrutinizing data breach incidents, and reviewing privacy policies to identify discrepancies or areas of concern. Leverage

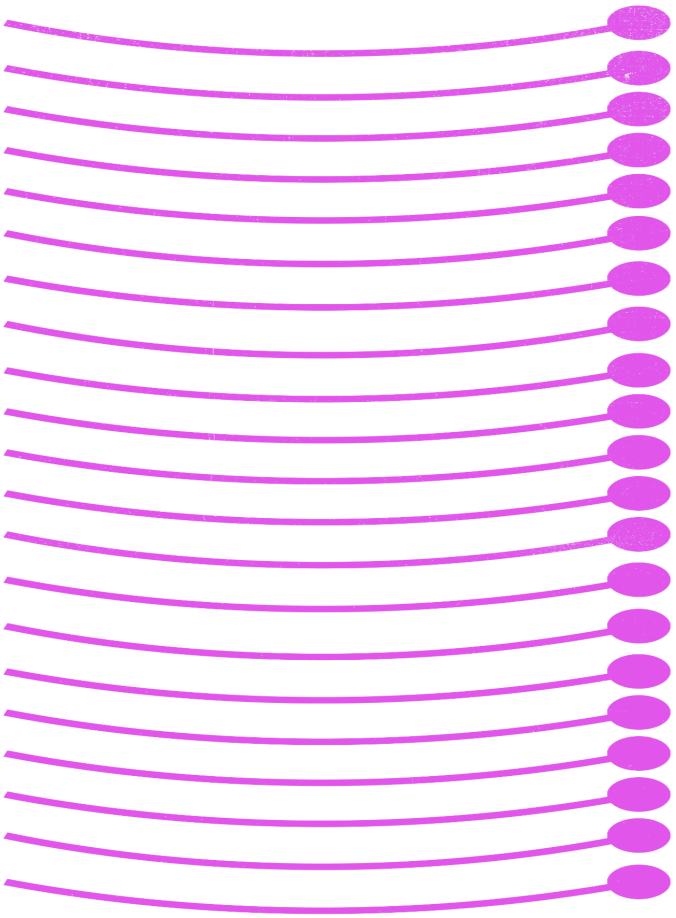
emerging technology solutions, such as automated monitoring tools, to systematically track compliance over time. Publicly and regularly disclose findings to educate consumers, pressure non-compliant companies to improve, and alert regulators to potential violations. Collaborate with regulatory bodies to influence future regulations and compliance frameworks, enhancing overall data privacy protections.

4.3. Recommendations for technology industry representatives

◇ **Prioritize privacy-enhancing technologies to bolster data security and to increase trust in your services.** Invest in research and development of tools such as encryption, anonymization, and decentralized data management systems, which not only protect user data but also enhance consumer trust. By leading advancements in privacy tech, address growing consumer concerns over data breaches and misuse. invest in robust data security infrastructures to protect against cyber threats and ensure the integrity of user data. Adopt state-of-the-art security protocols, conduct regular security audits, and educate employees on best practices for data protection (Skalkos et al, 2021, Baig et al, 2023).

◇ **Ensure meaningful consent mechanisms by leveraging human-centric design principles.** Develop intuitive and human-centric consent processes that offer users clear, understandable options regarding data collection, allowing them to make truly informed decisions. Opting out of data collection must be a straightforward and viable choice with no negative repercussions, empowering users without compromising their experience. Clearly articulate the purposes for which body-related data is collected and ensure practices do not exceed these stated purposes without additional consent or justification. This also includes extending beyond essential cookies and providing consumers with a truly tracking-free advertising option, thereby reducing reliance on intrusive business models (Allied Media Project: Building Consentful Tech Zine, 2017).

◇ **Practice data minimization and other responsible data practices as fundamental principles guiding your data collection mechanisms.** Limit your data collection to only what is necessary for specific functions and purposes. Conduct thorough and regular assessments to identify what specific data is essential for your services to function effectively, thereby eliminating the habitual over-collection of information. Implement stringent internal review processes to ensure that each data point collected has a justified purpose and concrete rationale for its retention. Develop and enforce clear responsible data handling policies that dictate not only what data is collected, but also how long it will be retained.



This includes setting automated data purging processes that regularly eliminate information that is no longer useful, reducing the risks associated with data breaches and mismanagement. Establish due diligence practices to ensure that third-party partners comply with relevant privacy standards and organizational policies regarding data handling (Responsible Data Forum, 2024).

◇ **When engaging in data-driven experimentations, align more closely with the ethical standards and practices found in clinical trials and behavioral research.** This involves integrating rigorous ethical review processes similar to Institutional Review Boards (IRBs) to assess the potential impacts and ethical considerations of data-driven experiments long before they are conducted. Just as participants in clinical trials are informed of risks and benefits, digital users should be made fully aware of how their data will be used and monetized, allowing them to make informed decisions about participation. This consent process should be ongoing, providing users with the ability to withdraw consent at any stage without penalty.

4.4. Recommendations for individual users

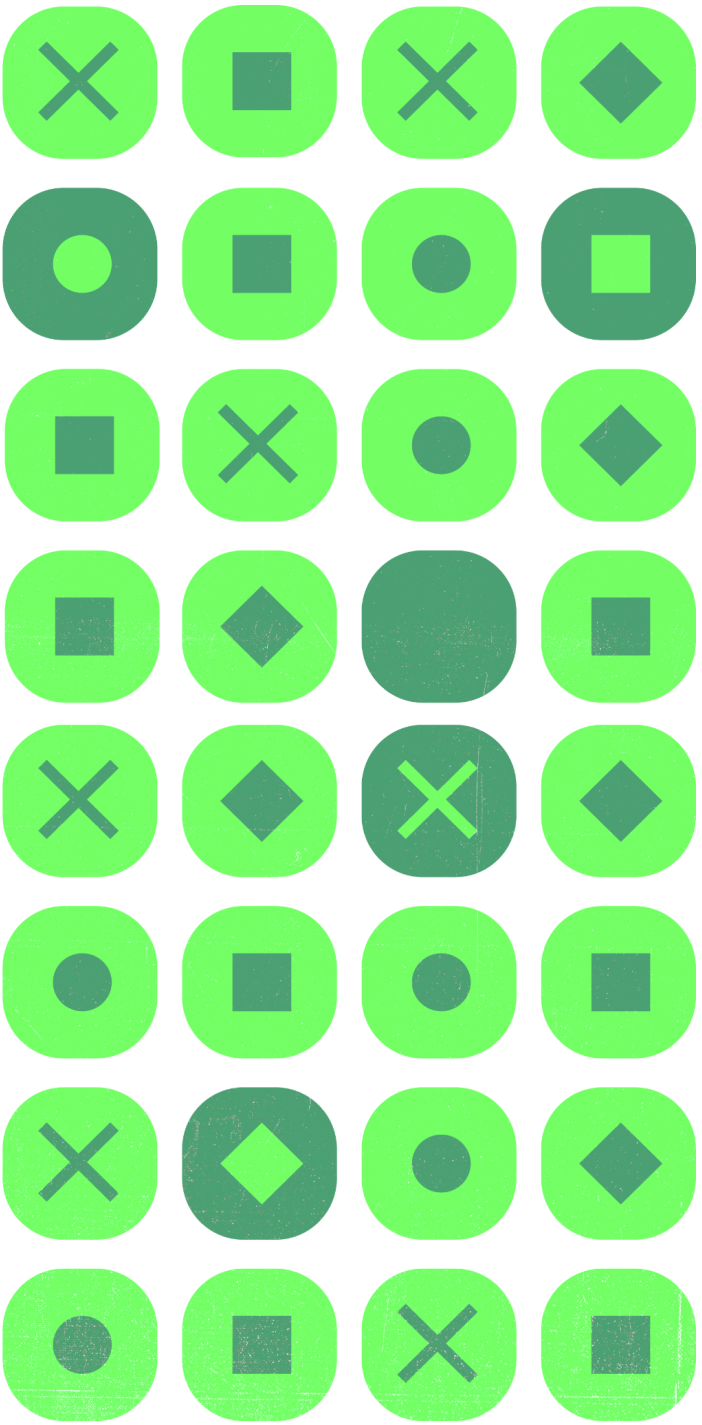
◇ **Prioritize privacy when sharing any type of information about your bodily and mental characteristics:** When sharing your bodily data, it is crucial to prioritize privacy by thoroughly evaluating the implications of your decisions. Leverage resources such as Mozilla's Privacy Not Included (PNI) to assess the privacy practices and data policies of health-related applications and devices you intend to use. By choosing technologies that meaningfully integrate user consent, transparency, and robust data protection measures, data policies of health-related applications and data policies of health-related applications and devices you intend to use. By choosing technologies that meaningfully integrate user consent, transparency, and robust data protection measures, you can significantly mitigate the risks associated with unauthorized data access and ensure that your personal information remains secure while benefiting from innovative digital health solutions.

◇ **Maintain a healthy security routine:** Establishing and adhering to a strong security routine on your devices is essential for safeguarding your bodily data from potential breaches. Regularly update your software, including applications and operating systems, to patch vulnerabilities that cybercriminals may exploit. Implement strong, unique passwords for each of your accounts, and enable two-factor authentication whenever available. These practices will create multiple layers of security, enhancing your overall data protection and making it significantly more challenging for unauthorized individuals to gain access to your sensitive information.

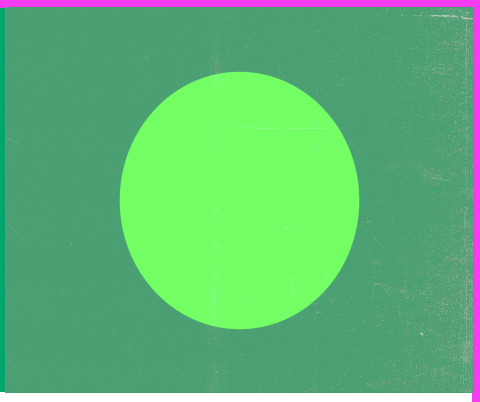
◇ **Stay informed about cybersecurity incidents:** Staying informed about the latest cybersecurity threats and incidents is vital for making informed decisions regarding your bodily data. Follow reputable news sources, cybersecurity blogs, and industry publications to keep track of breaches affecting technologies that collect and process health information. This continuous awareness enables you to critically evaluate the security measures of the services you use and make necessary adjustments to your data-sharing practices, ultimately enhancing your ability to protect your privacy in a rapidly evolving technological landscape.

◇ **Review data permissions regularly:** Regularly reviewing and managing the data permissions of the applications and devices you use is a proactive approach to protecting your privacy. Take time to assess which permissions have been granted for location tracking, health metrics access, and personal information sharing across your apps.

By proactively revoking unnecessary permissions that allow access to your sensitive data, you can better control how your bodily information is utilized. This vigilance helps limit your exposure and reinforces your commitment to maintaining privacy, ensuring that your personal data is only shared when absolutely necessary and with full understanding of its implications.



Bibliography



Addis, Adeno. "Dignity, Integrity, and the Concept of a Person." ICL Journal, vol. 13, no. 4, Dec. 2019, pp. 323–72.

Adler-Milstein, Julia, and Ashish K. Jha. "HITECH Act Drove Large Gains In Hospital Electronic Health Record Adoption." Health Affairs, vol. 36, no. 8, Aug. 2017, pp. 1416–22.

Akhand, M. a. H., et al. "Facial Emotion Recognition Using Transfer Learning in the Deep CNN." Electronics, vol. 10, no. 9, Jan. 2021, p. 1036.

Alekseenko, Aleksandra. "Implications for COVID-19 Vaccination Following the European Court of Human Right's Decision in Vavřička and Oths v Czech." Medical Law International, vol. 22, no. 1, Mar. 2022, pp. 75–89.

Alfawzan, Najd, et al. "Privacy, Data Sharing, and Data Security Policies of Women's mHealth Apps: Scoping Review and Content Analysis." JMIR mHealth and uHealth, vol. 10, no. 5, May 2022, p. e33735.

Algorithm-Driven Hiring Tools: Innovative Recruitment or Expedited Disability Discrimination? The Center for Democracy & Technology, Dec. 2020.

Aljedaani, Bakheet, et al. "End-Users' Knowledge and Perception about Security of Clinical Mobile Health Apps: A Case Study with Two Saudi Arabian mHealth Providers." Journal of Systems and Software, vol. 195, Jan. 2023, p. 111519.

Allen, Marshall. "Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates." ProPublica, 17 July 2018.

Alswaidan, Nourah, and Mohamed El Bachir Menai. "A Survey of State-of-the-Art Approaches for Emotion Recognition in Text." Knowledge and Information Systems, vol. 62, no. 8, Aug. 2020, pp. 2937–87.

Amagai, Saki, et al. "Challenges in Participant Engagement and Retention Using Mobile Health Apps: Literature Review." Journal of Medical Internet Research, vol. 24, no. 4, Apr. 2022, p. e35120.

Andrews, Mel, et al. "The Reanimation of Pseudoscience in Machine Learning and Its Ethical Repercussions." Patterns, vol. 5, no. 9, Sept. 2024, p. 101027.

Angwin, Julia, et al. "Machine Bias." ProPublica, 23 May 2016.

Annas, George J., and Michael A. Grodin. "Medical Ethics and Human Rights: Legacies of Nuremberg." Hofstra Law and Policy Symposium, vol. 3, 1999, p. 111.

Arai-Yokoi, Yutaka. "Grading Scale Of Degradation: Identifying The Threshold Of Degrading Treatment Or Punishment Under Article 3 ECHR." Netherlands Quarterly of Human Rights, vol. 21, no. 3, 2003, pp. 385–421.

Armitage, Catherine, et al. Study on the Impact of Recent Developments in Digital Advertising on Privacy, Publishers and Advertisers. Publications Office of the European Union, 2023.

Aswathy, S. U., and Amit Kumar Tyagi. "Privacy Breaches through Cyber Vulnerabilities: Critical Issues, Open Challenges, and Possible Countermeasures for the Future." Security and Privacy-Preserving Techniques in Wireless Robotics, CRC Press, 2022.

Atlas of eHealth Country Profiles. WHO Global Observatory for eHealth, 2016.

Awad, Ali Ismail, et al. "AI-Powered Biometrics for Internet of Things Security: A Review and Future Vision." Journal of Information Security and Applications, vol. 82, May 2024, p. 103748.

Ayeswarya, S., and K. John Singh. "A Comprehensive Review on Secure Biometric-Based Continuous Authentication and User Profiling." IEEE Access, vol. 12, 2024, pp. 82996–3021.

Baig, Ahmed Fraz, et al. "Privacy-Preserving Continuous Authentication Using Behavioral Biometrics." International Journal of Information Security, vol. 22, no. 6, Dec. 2023, pp. 1833–47.

Bak, Marieke, et al. "You Can't Have AI Both Ways: Balancing Health Data Privacy and Access Fairly." Frontiers in Genetics, vol. 13, June 2022.

Bakare, Seun Solomon, et al. "Data Privacy Laws And Compliance: A Comparative Review Of The EU GDPR And USA Regulations." Computer Science & IT Research Journal, vol. 5, no. 3, Mar. 2024, pp. 528–43.

Baron, Benjamin, and Mirco Musolesi. "Where You Go Matters: A Study on the Privacy Implications of Continuous Location Tracking." Proc. ACM Interact. Mob. Wearable Ubiquitous Technol., vol. 4, no. 4, Dec. 2020, p. 169:1-169:32.

Barr, Shoshana Wodinsky &. Kyle. "These Companies Know When You're Pregnant—And They're Not Keeping It Secret." Gizmodo, 30 July 2022.

Basil, Nduma N., et al. "Health Records Database and Inherent Security Concerns: A Review of the Literature." Cureus, vol. 14, no. 10, p. e30168. Accessed 2 Oct. 2024.

Bassiouni, M. Cherif. "Introduction to International Criminal Law, 2nd Revised Edition." Introduction to International Criminal Law, 2nd Revised Edition, Brill Nijhoff, 2013.

Baxter, Teri Dobbins. Child Sacrifices: The Precarity of Minors' Autonomy and Bodily Integrity After Dobbs. 4802815, 13 Apr. 2024.

Beduschi, Ana. "Synthetic Data Protection: Towards a Paradigm Change in Data Regulation?" Big Data & Society, vol. 11, no. 1, Mar. 2024.

Beetham, Helen, et al. "Surveillance Practices, Risks and Responses in the Post Pandemic University." Digital Culture and Education, vol. 14, no. 1, Feb. 2022, pp. 16–37.

Berggren, C., and J. Wrangborg. Constant Surveillance at Work: Prevalence and Consequences of Monitoring in Commerce. Swedish Commercial Employees' Union , Nov. 2022.

Bernal, Paul. "Our Web History Reveals What We Think and Do. Shouldn't That Remain Private?" The Conversation, 9 Nov. 2015.

Beyond Face Value: Public Attitudes to Facial Recognition Technology. Ada Lovelace Institute , Sept. 2019.

Bhuiyan, Johana. "Google Promised to Delete Location Data on Abortion Clinic Visits. It Didn't, Study Says." The Guardian, 17 Jan. 2024.

Bincoletto, Giorgia. "Data Protection Issues in Cross-Border Interoperability of Electronic Health Record Systems within the European Union." Data & Policy, vol. 2, Jan. 2020, p. e3.

Biometric System Market Size, Share, Trends and Growth Analysis 2032. Markets and Markets. Accessed 18 Nov. 2024.

Biometric Technology Market Size & Share Report, 2030. Grand View Research. Accessed 18 Nov. 2024.

Blanke, Jordan M. "Protection for 'Inferences Drawn': A Comparison Between the General Data Protection Regulation and the California Consumer Privacy Act." Global Privacy Law Review, vol. 1, no. 2, June 2020.

Bonomi, Luca, et al. "Privacy Challenges and Research Opportunities for Genomic Data Sharing." Nature Genetics, vol. 52, no. 7, July 2020, pp. 646–54.

Botta, Marco, and Danielle Borges. "User Consent at the Interface of the DMA and the GDPR. A Privacy-Setting Solution to Ensure Compliance with ART. 5(2) DMA." Robert Schuman Centre for Advanced Studies Research Paper, vol. No. 2023_68, Dec. 2023.

"British Columbia Lawsuit Claims Flo Health Shared Personal Data with Facebook." IAPP, Mar. 2024.

Buolamwini, Joy, and Timnit Gebru. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." Proceedings of Machine Learning Research 81:1–15, 2018, 2018.

Cabitza, Federico, et al. "The Unbearable (Technical) Unreliability of Automated Facial Emotion Recognition." Big Data & Society, vol. 9, no. 2, July 2022.

Callanan, Gerard A., et al. "Targeting Vulnerable Populations: The Ethical Implications of Data Mining, Automated Prediction, and Focused Marketing." Business and Society Review, vol. 126, no. 2, June 2021, pp. 155–67.

Callier, Shawneequa, and Stephanie M. Fullerton. "Diversity and Inclusion in Unregulated mHealth Research: Addressing the Risks." Journal of Law, Medicine & Ethics, vol. 48, no. S1, 2020, pp. 115–21.

Caltrider, Jen, et al. Romantic AI Chatbots Don't Have Your Privacy at Heart. Mozilla Foundation, 14 Feb. 2024.

Carmi, Lior, et al. "The European General Data Protection Regulation (GDPR) in mHealth: Theoretical and Practical Aspects for Practitioners' Use." Medicine, Science and the Law, vol. 63, no. 1, Jan. 2023, pp. 61–68.

Chiarella, Maria Luisa. "Digital Markets Act (DMA) and Digital Services Act (DSA): New Rules for the EU Digital Environment." Athens Journal of Law (AJL), vol. 9, 2023, p. 33.

Chong, Heather. "Data for Sale: Navigating the Role of Data Brokers and Reproductive Health Information in a Post-Dobbs World." SMU Science and Technology Law Review, vol. 26, 2023, p. 99.

Church, Christopher E., and Amanda J. Fairchild. "In Search of a Silver Bullet: Child Welfare's Embrace of Predictive Analytics." Juvenile and Family Court Journal, vol. 68, no. 1, Mar. 2017, pp. 67–81.

Citron, Danielle. The Fight for Privacy: Protecting Dignity, Identity and Love in Our Digital Age. W. W. Norton & Company, 2022.

Clayton, Ellen Wright, et al. "Dobbs and the Future of Health Data Privacy for Patients and Healthcare Organizations." Journal of the American Medical Informatics Association , vol. 30, no. 1, Jan. 2023, pp. 155–60.

Cox, Joseph. "Data Marketplace Selling Info About Who Uses Period Tracking Apps." VICE, 17 May 2022.

---. "FTC Fines Avast $16.5 Million For Selling Browsing Data Harvested by Antivirus." 404 Media, 22 Feb. 2024.

Custers, Bart, and Gianclaudio Malgieri. "Priceless Data: Why the EU Fundamental Right to Data Protection Is at Odds with Trade in Personal Data." Computer Law & Security Review, vol. 45, July 2022, p. 105683.

D'Alfonso, Simon. "AI in Mental Health." Current Opinion in Psychology, vol. 36, Dec. 2020, pp. 112–17.

Data Broker Market Size & Share: Industry Report, 2024 - 2029. Knowledge Sourcing Intelligence LLP. Accessed 18 Nov. 2024.

Data Broker Market Size, Share, Industry Growth 2032. Market Research Future. Accessed 18 Nov. 2024.

De Keyser, Arne, et al. "Opportunities and Challenges of Using Biometrics for Business: Developing a Research Agenda." Journal of Business Research, vol. 136, Nov. 2021, pp. 52–62.

Demopoulos, Alaina. "'There Are No Serious Safeguards': Can 23andMe Be Trusted with Our DNA?" The Guardian, 17 Feb. 2024.

Deniz-Garcia, Alejandro, et al. "Quality, Usability, and Effectiveness of mHealth Apps and the Role of Artificial Intelligence: Current Scenario and Challenges." Journal of Medical Internet Research, vol. 25, no. 1, May 2023, p. e44030.

Devkota, Mahadev. "The Privacy Price of School Safety Stakeholders' Perceptions Towards the Use of Closed-Circuit Television (CCTV) in Schools." Madhyabindu Journal, vol. 9, May 2024.

Dhondt, Karel, et al. "A Run a Day Won't Keep the Hacker Away: Inference Attacks on Endpoint Privacy Zones in Fitness Tracking Social Networks." CCS '22: Proceedings of the 2022 ACM SIGSAC, 2022, pp. 801–14.

Diamant, Dana. "Top 5 Cyber Attacks That Target Patient Privacy in mHealth Apps." Appdome, 27 Sept. 2022.

Dicke, Klaus. "The Founding Function of Human Dignity in the Universal Declaration of Human Rights." The Concept of Human Dignity in Human Rights Discourse, Brill Nijhoff, 2001, pp. 111–20, https://doi.org/10.1163/9789004478190_008.

"Digital Rights Are Charter Rights." Digital Freedom Fund. Accessed 18 Nov. 2024.

Donnelly, Jack, and Daniel J. Whelan. International Human Rights. 6th ed., Routledge, 2020.

Douglas, Thomas, and Lisa Forsberg. "Three Rationales for a Legal Right to Mental Integrity." Neurolaw: Advances in Neuroscience, Justice & Security, edited by Sjors Ligthart et al., Springer International Publishing, 2021, pp. 179–201.

Duivenvoorde, Bram, and Catalina Goanta. "The Regulation of Digital Advertising under the DSA: A Critical Assessment." Computer Law & Security Review, vol. 51, Nov. 2023, p. 105870.

Duncan, Jamie. "Data Protection beyond Data Rights: Governing Data Production through Collective Intermediaries." Internet Policy Review, vol. 12, no. 3, Sept. 2023.

Dworkin, Ronald. Law's Empire. Harvard University Press, 1986.

Electronic Health Record Market Size & Share Report, 2032. Global Market Insights. Accessed 7 Nov. 2024.

Electronic Health Records [EHR] Market Size & Share, 2032. Fortune Business Insights. Accessed 7 Nov. 2024.

Electronic Health Records Market Size & Share Report, 2030. Grand View Research. Accessed 7 Nov. 2024.

Electronic Health Records Market Size to Hit USD 44.39 Billion by 2034. Precedence Research. Accessed 7 Nov. 2024.

Eubanks, Virginia. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor Hardcover – January 23, 2018. St. Martin's Press, 2018.

European Health Union: A European Health Data Space for People and Science. European Commission, May 2022.

Fabrègue, Brian F. G., and Andrea Bogoni. "Privacy and Security Concerns in the Smart City." Smart Cities, vol. 6, no. 1, Feb. 2023, pp. 586–613.

Falcetta, Frederico Soares, et al. "Automatic Documentation of Professional Health Interactions: A Systematic Review." Artificial Intelligence in Medicine, vol. 137, Mar. 2023, p. 102487.

Farinho, Domingos Soares. "Personal Data Processing by Online Platforms and Search Engines: The Case of the EU Digital Services Act." Public Governance, Administration and Finances Law Review (PGAF LR), vol. 9, 2024, p. 37.

Feldman Barrett, Lisa, et al. "Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements." Psychol Sci Public Interest, vol. 20:, no. 1, July 2019, pp. 1–68.

Finck, Pallas. “They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR .” International Data Privacy Law, vol. 10, no. 1, Feb. 2020, pp. 11–36.

Flynn, Maria, et al. “Assessing the Effectiveness of Automated Emotion Recognition in Adults and Children for Clinical Investigation.” Frontiers in Human Neuroscience, vol. 14, Apr. 2020, p. 70.

Fortmeyer, Robert. Guardians of Biometrics: Navigating the Corporate Responsibility to Biometric Data in the Digital Age. 4703857, 30 Nov. 2023.

Frewer, Andreas. “Human Rights from the Nuremberg Doctors Trial to the Geneva Declaration. Persons and Institutions in Medical Ethics and History.” Medicine, Health Care and Philosophy, vol. 13, no. 3, Aug. 2010, pp. 259–68.

FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data. Federal Trade Commission, 9 Jan. 2024.

Gak, Liza, et al. “The Distressing Ads That Persist: Uncovering The Harms of Targeted Weight-Loss Ads Among Users with Histories of Disordered Eating.” Proceedings of the ACM on Human-Computer Interaction, vol. 6, no. CSCW2, Nov. 2022, p. 377:1-377:23.

Galetsi, Panagiota, et al. “Exploring Benefits and Ethical Challenges in the Rise of mHealth (Mobile Healthcare) Technology for the Common Good: An Analysis of Mobile Applications for Health Specialists.” Technovation, vol. 121, Mar. 2023, p. 102598.

Gallin, Stacy, and Ira Bedzow. “Holocaust as an Inflection Point in the Development of Bioethics and Research Ethics.” Handbook of Research Ethics and Scientific Integrity, edited by Ron Iphofen, Springer International Publishing, 2020, pp. 1071–90.

Gentile, Giulia, and Orla Lynskey. “Deficient By Design? The Transnational Enforcement Of The GDPR.” International & Comparative Law Quarterly, vol. 71, no. 4, Oct. 2022, pp. 799–830.

“Global Pharmaceutical Industry - Statistics & Facts.” Statista. Accessed 18 Nov. 2024.

Goldstein; Alonso-Bejarano. “E-Terrify: Securitized Immigration and Biometric Surveillance in the Workplace .” Human Organization: Journal of the Society for Applied Anthropology, vol. Anthropology of Immigration, no. 76, Mar. 2017, pp. 1–14.

Gronowski, Ann, et al. “Ethics for Laboratory Medicine .” Clinical Chemistry, vol. 65, no. 12, Dec. 2019, pp. 1497–507.

Grundy, Quinn. “A Review of the Quality and Impact of Mobile Health Apps.” Annual Review of Public Health, vol. 43, no. 1, Apr. 2022, pp. 117–34.

Guay, Rob, and Kean Birch. “A Comparative Analysis of Data Governance: Socio-Technical Imaginaries of Digital Personal Data in the USA and EU (2008–2016).” Big Data & Society, vol. 9, no. 2, July 2022.

Guillou-Landreat, Morgane, et al. “Gambling Marketing Strategies and the Internet: What Do We Know? A Systematic Review.” Frontiers in Psychiatry, vol. 12, Feb. 2021.

Guo, Eileen, and Hikmat Noori. “This Is the Real Story of the Afghan Biometric Databases Abandoned to the Taliban.” MIT Technology Review, Aug. 2021.

Hamdoun, Salah, et al. “AI-Based and Digital Mental Health Apps: Balancing Need and Risk.” IEEE Technology and Society Magazine, vol. 42, no. 1, Mar. 2023, pp. 25–36.

Hamzelou, Jessica. “A New Law in California Protects Consumers’ Brain Data. Some Think It Doesn’t Go Far Enough.” MIT Technology Review. Accessed 18 Nov. 2024.

Hanus, Andrea. “Privacy for Sale: How the FTC Can Take Precise Location Data Off the Market.” Boston University Law Review, vol. 104, no. 2, Apr. 2024, p. 655.

Haque, M. D. Romael, and Sabirat Rubya. “An Overview of Chatbot-Based Mobile Mental Health Apps: Insights From App Description and User Reviews.” JMIR mHealth and uHealth, vol. 11, no. 1, May 2023.

Hart, Robert. “Clearview AI Fined $9.4 Million In U.K. For Illegal Facial Recognition Database.” Forbes. Accessed 18 Nov. 2024.

Health Threat Landscape. Report/Study, European Union Agency for Cybersecurity (ENISA) . Accessed 18 Nov. 2024.

Healthcare Data Breach Statistics. The HIPAA Journal, 24 Oct. 2024.

Healy, Rachael Louise. “Zuckerberg, Get out of My Uterus! An Examination of Fertility Apps, Data-Sharing and Remaking the Female Body as a Digitalized Reproductive Subject.” Journal of Gender Studies, vol. 30, no. 4, May 2021, pp. 406–16.

Heller, Brittan. “Reimagining Reality: Human Rights and Immersive Technology.” Harvard Carr Center Discussion Paper Series, 2020.

---. “Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law.” Vanderbilt Journal of Entertainment & Technology Law, vol. 23, 2021 2020, p. 1.

Hendel, John. “Crisis Text Line Ends Data-Sharing Relationship with for-Profit Spinoff.” Politico, 31 Jan. 2022.

Herring, Jonathan, and Jesse Wall. "The Nature And Significance Of The Right To Bodily Integrity." The Cambridge Law Journal, vol. 76, no. 3, Nov. 2017, pp. 566–88.

Hill, Kashmir. "How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did." Forbes. Accessed 18 Nov. 2024.

Hill, Kashmir, and Aaron Krolik. "At Talkspace, Start-Up Culture Collides With Mental Health Concerns." The New York Times, 7 Aug. 2020.

Hossain, Elias, et al. "Natural Language Processing in Electronic Health Records in Relation to Healthcare Decision-Making: A Systematic Review." Computers in Biology and Medicine, vol. 155, Mar. 2023, p. 106649.

Huddleston, Ashley, and Ronald Hedges. "Liability for Health Care Providers under HIPAA and State Privacy Laws." Seton Hall Law Review, vol. 51, 2021 2020, p. 1585.

Human Rights Watch. UN Shared Rohingya Data Without Informed Consent. 15 June 2021.

Hussain, Altaf, et al. "AI-Driven Behavior Biometrics Framework for Robust Human Activity Recognition in Surveillance Systems." Engineering Applications of Artificial Intelligence, vol. 127, Jan. 2024, p. 107218.

Ienca, Marcello. "On Neurorights." Frontiers in Human Neuroscience, vol. 15, Sept. 2021.

Ignovska, Elena. "Mandatory Vaccination Against COVID-19 in Europe: Public Health Versus 'Saved by the Bell' Individual Autonomy." Modernising European Legal Education, 2023, pp. 283–303.

Institute, AI Now. Regulating Biometrics: Global Approaches and Open Questions. 1 Sept. 2020.

Ioannou, Athina, et al. "Privacy Concerns and Disclosure of Biometric and Behavioral Data for Travel." International Journal of Information Management, vol. 54, Oct. 2020, p. 102122.

Iwaya, Leonardo Horn, et al. "On the Privacy of Mental Health Apps: An Empirical Investigation and Its Implications for App Development." Empirical Softw. Engg., vol. 28, no. 1, Nov. 2022.

Jacobsen, Katja Lindskov. "Biometric Data Flows and Unintended Consequences of Counterterrorism." International Review of the Red Cross, vol. 103, no. 916–917, Apr. 2021, pp. 619–52.

Jain, Mardav. The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment. The Henry M. Jackson School of International Studies, 9 May 2019.

Jang, Sooah, et al. "Mobile App-Based Chatbot to Deliver Cognitive Behavioral Therapy and Psychoeducation for Adults with Attention Deficit: A Development and Feasibility/Usability Study." International Journal of Medical Informatics, vol. 150, June 2021.

Javaid, Mohd, et al. "Towards Insighting Cybersecurity for Healthcare Domains: A Comprehensive Review of Recent Practices and Trends." Cyber Security and Applications, vol. 1, Dec. 2023, p. 100016.

Kalckreuth, Niklas von, and Markus A. Feufel. "Extending the Privacy Calculus to the mHealth Domain: Survey Study on the Intention to Use mHealth Apps in Germany." JMIR Human Factors, vol. 10, no. 1, Aug. 2023.

Kanwal, Rahul, and Kevin Walby. Tracking the Surveillance and Information Practices of Data Brokers. Winnipeg, MB: Centre for Access to Information and Justice, 4 July 2024.

Kaplan, Bonnie. "PHI Protection under HIPAA: An Overall Analysis." São Paulo: Editora Revista Dos Tribunais (Thomsom Reuters), May 2021, pp. 61–88.

Keegan, Jon, and Joel Eastwood. From "Heavy Purchasers" of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You. The Markup, 8 June 2023.

Kessel, Robin van, Madeleine Haig, et al. "Strengthening Cybersecurity for Patient Data Protection in Europe." Journal of Medical Internet Research, vol. 25, Aug. 2023.

Kessel, Robin van, Ilias Kyriopoulos, et al. "The Effect of the COVID-19 Pandemic on Digital Health–Seeking Behavior: Big Data Interrupted Time-Series Analysis of Google Trends." Journal of Medical Internet Research, vol. 25, no. 1, Jan. 2023.

Khan, Z. Faizal, and Sultan Refa Alotaibi. "Applications of Artificial Intelligence and Big Data Analytics in M-Health: A Healthcare System Perspective." Journal of Healthcare Engineering, vol. 2020, Sept. 2020, pp. 1–15.

Khare, Smith K., et al. "Emotion Recognition and Artificial Intelligence: A Systematic Review (2014–2023) and Research Recommendations." Information Fusion, vol. 102, Feb. 2024.

Killoran, Jayson, et al. "Can Behavioral Biometrics Make Everyone Happy?" Business Horizons, vol. 66, no. 5, Sept. 2023, pp. 585–91.

Kim, Joanne. Data Brokers and the Sale of Americans' Mental Health Data. Duke Sanford Cyber Policy Program, Feb. 2023.

Kingston, Lindsey N. "Biometric Identification, Displacement, and Protection Gaps ." Digital Lifeline?: ICTs for Refugees and Displaced Persons, The MIT Press, 2018.

Knight, Alissa. "All That We Let In: Hacking Mobile Health APIs (Part 1)." Medium, 1 Dec. 2020.

Kovacic, William. "Adaptable Platforms for Platform Regulation: The Role of the Federal Trade Commission." Journal of Law & Innovation, vol. 7, no. 1, Aug. 2024, pp. 106–33.

Kovacs, Anja, and Tripti Jain. "Informed Consent - Said Who? A Feminist Perspective on Principles of Consent in the Age of Embodied Data." SSRN, Mar. 2021.

Lagerkvist, Amanda, et al. "Body Stakes: An Existential Ethics of Care in Living with Biometrics and AI." AI & SOCIETY, vol. 39, no. 1, Feb. 2024, pp. 169–81.

Lawson, Alex. "Sainsbury's Boss Defends Decision to Sell Customers' Nectar Card Data." The Guardian, 13 Dec. 2023.

Leufer, Daniel. Bodily Harms: Mapping the Risks of Emerging Biometric Tech. Access Now, Oct. 2023.

Lewis , Abigail, et al. "Electronic Health Record Data Quality Assessment and Tools: A Systematic Review ." Journal of the American Medical Informatics Association, vol. 30, no. 10, pp. 1730–40. Accessed 18 Nov. 2024.

Lewis, Abigail E., et al. "Electronic Health Record Data Quality Assessment and Tools: A Systematic Review." Journal of the American Medical Informatics Association, vol. 30, no. 10, Oct. 2023, pp. 1730–40.

Ligthart, Sjors. "Towards a Human Right to Psychological Continuity? Reflections on the Rights to Personal Identity, Self-Determination, and Personal Integrity." European Convention on Human Rights Law Review, The, vol. 5, no. 2, Apr. 2024, pp. 199–229.

López Martínez, Antonio, et al. "A Comprehensive Review of the State-of-the-Art on Security and Privacy Issues in Healthcare." ACM Comput. Surv., vol. 55, no. 12, Mar. 2023, p. 249:1-249:38.

Lucia, Cascone, et al. "Biometrics for Industry 4.0: A Survey of Recent Applications." Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 8, Aug. 2023, pp. 11239–61.

Madianou, Mirca. "The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies." Television & New Media, vol. 20, no. 6, Sept. 2019, pp. 581–99.

Marani, Mehdi, et al. "The Role of Biometric in Banking: A Review." EAI Endorsed Transactions on AI and Robotics, vol. 2, no. 1, Aug. 2023.

Masuch, Kristin, et al. "Fitness First or Safety First? Examining Adverse Consequences of Privacy Seals in the Event of a Data Breach." 54th Hawaii International Conference on System Sciences, 2021.

Mehrnezhad, Maryam, and Teresa Almeida. "Caring for Intimate Data in Fertility Technologies." Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Association for Computing Machinery, 2021, pp. 1–11.

Meishar-Tal, Hagit, et al. "Implications of CCTV Cameras on Child-Care Centres' Routines, Peer Relationships, and Parent–Teacher Relationships: Child Care Educators' Opinions." International Journal of Child Care and Education Policy, vol. 16, no. 1, Oct. 2022, p. 9.

Mendolla, Mackenzie K. "A Blurry Lens: Assessing the Complicated Legal Landscape of Biometric Privacy through the Perspective of Mobile Apps." Seton Hall Law Review, vol. 54, 2024 2023, p. 923.

mHealth Market Size, Share & Growth Analysis Report 2030. Grand View Research. Accessed 18 Nov. 2024.

mHealth Market Size, Share & Value . Fortune Business Insights. Accessed 18 Nov. 2024.

mHealth Market Size, Share, Growth Insight by 2031. Transparency Market Research. Accessed 18 Nov. 2024.

mHealth Market Size to Hit Around USD 268.46 Billion by 2034. Precedence Research. Accessed 18 Nov. 2024.

Micheli, Marina, et al. "Mapping the Landscape of Data Intermediaries." JRC Publications Repository, 24 Aug. 2023.

Minssen, Timo, et al. "Governing AI in the European Union: Emerging Infrastructures and Regulatory Ecosystems in Health." Research Handbook on Health, AI and the Law, Edward Elgar Publishing, 2024, pp. 311–31.

Molnar, Petra. "Territorial and Digital Borders and Migrant Vulnerability Under a Pandemic Crisis." Migration and Pandemics, Springer, 2021, pp. 45–64.

Moriuchi, Emi. "An Empirical Study of Consumers' Intention to Use Biometric Facial Recognition as a Payment Method." Psychology & Marketing, vol. 38, no. 10, Oct. 2021, pp. 1741–65.

Morrison, Sara. "The Hidden Trackers in Your Phone, Explained." Vox, 8 July 2020.

Nagai, Hiroyuki, et al. "The Creation of the Belmont Report and Its Effect on Ethical Principles: A Historical Study." Monash Bioethics Review, vol. 40, no. 2, Dec. 2022, pp. 157–70.

Negro-Calduch, Elsa, et al. "Technological Progress in Electronic Health Record System Optimization: Systematic Review of Systematic Literature Reviews." International Journal of Medical Informatics, vol. 152, Aug. 2021, p. 104507.

Nema, Purvi. "Privacy And Security Concerns In Electronic Health Records - A Comparative Study Between India And USA." Centre for Socio Legal Research , vol. 1, no. 1, 2021.

Niki, O'Brien, et al. "Cyber-Attacks Are a Permanent and Substantial Threat to Health Systems: Education Must Reflect That." DIGITAL HEALTH, vol. 8, Jan. 2022, p. 205520762211046.

Nwano, Theophilus, and Lilian Akhirome-Omonfuegbe. "Roe v Wade and the Global Whirlwind Implications on Women's Reproductive Rights." Journal of Law, Policy and Globalization, vol. 141, 2024, p. 91.

"Of 42 'Hunger-Related' Deaths Since 2017, 25 'Linked to Aadhaar Issues.'" The Wire. Accessed 18 Nov. 2024.

Oh, Jooyoung, et al. "Efficacy of Mobile App-Based Interactive Cognitive Behavioral Therapy Using a Chatbot for Panic Disorder." International Journal of Medical Informatics, vol. 140, Aug. 2020, p. 104171.

Olawade, David B., et al. "Enhancing Mental Health with Artificial Intelligence: Current Trends and Future Prospects." Journal of Medicine, Surgery, and Public Health, vol. 3, Aug. 2024, p. 100099.

Omaghomi, Toritsemogba Tosanbami, et al. "Health Apps and Patient Engagement: A Review of Effectiveness and User Experience." World Journal of Advanced Research and Reviews, vol. 21, no. 2, 2024, pp. 432–40.

O'Sullivan, Lydia, et al. "Contributory Factors to the Evolution of the Concept and Practice of Informed Consent in Clinical Research: A Narrative Review." Contemporary Clinical Trials Communications, vol. 19, Sept. 2020, p. 100634.

Ozonze, Obinwa, et al. "Automating Electronic Health Record Data Quality Assessment." Journal of Medical Systems, vol. 47, no. 1, Feb. 2023, p. 23.

Palaniappan, Kavitha, et al. "Global Regulatory Frameworks for the Use of Artificial Intelligence (AI) in the Healthcare Services Sector." Healthcare, vol. 12, no. 5, Jan. 2024, p. 562.

Paltrow, Lynn M., et al. "Beyond Abortion: The Consequences of Overturning Roe." The American Journal of Bioethics, vol. 22, no. 8, Aug. 2022, pp. 3–15.

Patella-Rey, Pj. "Beyond Privacy: Bodily Integrity as an Alternative Framework for Understanding Non-Consensual Pornography." Information, Communication & Society, vol. 21, no. 5, May 2018, pp. 786–91.

Patterson, Dan, and Graham Kates. "We Found Our Personal Data on the Dark Web. Is Yours There, Too?" CBS News, 25 Mar. 2019.

Perlroth , Nicole, and Adam Satariano. "Irish Hospitals Are Latest to Be Hit by Ransomware Attacks." The New York Times, 20 May 2021.

Perosa, Teresa, and Quito Tsui. Biometrics in the Humanitarian Sector. The Engine Room, July 2023.

Perrin, Zoé, and Louise Mathieu. Citizens' Perception of and Engagement with Health Data Secondary Use and Sharing in Europe. TEHDAS, Nov. 2021.

Petersen, Carole J. "Women's Right to Equality and Reproductive Autonomy: The Impact of Dobbs v. Jackson Women's Health Organization." University of Hawai'i Law Review, vol. 45, 2023 2022, p. 305.

Popoola, Olusogo, et al. "A Critical Literature Review of Security and Privacy in Smart Home Healthcare Schemes Adopting IoT & Blockchain: Problems, Challenges and Solutions." Blockchain: Research and Applications, vol. 5, no. 2, June 2024, p. 100178.

Presthus, Wanda, and Kaja Felix Sønslien. "An Analysis of Violations and Sanctions Following the GDPR." International Journal of Information Systems and Project Management, vol. 9, no. 1, Jan. 2021, pp. 38–53.

Purdon, Lucy. Unfinished Business: Incorporating a Gender Perspective into Digital Advertising Reform in the UK and EU. Mozilla Foundation, Oct. 2023.

Raab, René. "Federated Electronic Health Records for the European Health Data Space." The Lancet Digital Health, vol. 5, no. 11, Nov. 2023, pp. e840–47.

Radhakrishnan, Radhika. Health Data as Wealth: Understanding Patient Rights in India within a Digital Ecosystem. Data Governance Network, Oct. 2021.

Rahman, Zara, and Júlia Keserű. Predictive Analytics for Children An Assessment of Ethical Considerations, Risks, and Benefits. UNICEF, Nov. 2021.

Rao, P. Muralidhara, and B. D. Deebak. "Security and Privacy Issues in Smart Cities/Industries: Technologies, Applications, and Challenges." Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 8, Aug. 2023, pp. 10517–53.

Rehman, Muhammad Haseeb. "Correlation of Workplace Surveillance with Psychological Health, Productivity, and Privacy of Employees." International Journal of Scientific & Engineering Research, vol. 13, no. 11, Nov. 2022.

Renieris, Elizabeth M. Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse. MIT Press, 2023.

"Report: Fitness Tracker Data Breach Exposed 61 Million Records and User Data Online." Website Planet, 13 Sept. 2021.

Resnik, Judith. "Judging Consent." University of Chicago Legal Forum, vol. 1987, 1987, p. 43.

Reviglio, Urbano. "The Untamed and Discreet Role of Data Brokers in Surveillance Capitalism: A Transnational and Interdisciplinary Overview." Internet Policy Review, vol. 11, no. 3, Aug. 2022.

Ritchie, Kay L., et al. "Public Attitudes towards the Use of Automatic Facial Recognition Technology in Criminal Justice Systems around the World." PLoS ONE, vol. 16, no. 10, Oct. 2021.

Rossmaier, Leon, et al. "Commercial mHealth Apps and the Providers' Responsibility for Hope." Digital Society, vol. 2, no. 3, Sept. 2023, p. 39.

Rossmaier, Leon W. S. "Commercial mHealth Apps and Unjust Value Trade-Offs: A Public Health Perspective." Public Health Ethics, vol. 15, no. 3, Sept. 2022, p. 277.

Ruohonen, Jukka, and Kalle Hjerppe. "The GDPR Enforcement Fines at Glance." Information Systems, vol. 106, May 2022, p. 101876.

Rupp, Valentin, and Max von Grafenstein. "Clarifying 'Personal Data' and the Role of Anonymisation in Data Protection Law." Computer Law & Security Review, vol. 52, Apr. 2024, p. 105932.

Ruschemeier, Hannah. "Data Brokers and European Digital Legislation." European Data Protection Law Review, vol. 9, no. 1, 2023, pp. 27–38.

Saha, Bilash. "Analysis of the Adherence of mHealth Applications to HIPAA Technical Safeguards." Master of Science in Information Technology Theses, Apr. 2023.

Sardar, Alamgir, et al. "A Secure Face Recognition for IoT-Enabled Healthcare System." ACM Trans. Sen. Netw., vol. 19, no. 3, Apr. 2023, p. 52:1-52:23.

Schipper, Irene, et al. "EU Legislation on Health Data a Gift to Big Tech." Social Europe, 20 Feb. 2024.

Schmidt, Jelena, et al. "Mapping the Regulatory Landscape for Artificial Intelligence in Health within the European Union." Npj Digital Medicine, vol. 7, no. 1, Aug. 2024, pp. 1–9.

Shah, Shahid Munir, and Rizwan Ahmed Khan. "Secondary Use of Electronic Health Record: Opportunities and Challenges." IEEE Access, vol. 8, 2020, pp. 136947–65.

Sharma, Mridula, and Haytham Elmiligi. "Behavioral Biometrics: Past, Present and Future." Recent Advances in Biometrics, IntechOpen, 2022.

Shipp, Laura, and Jorge Blasco. "How Private Is Your Period?: A Systematic Analysis of Menstrual App Privacy Policies." Proceedings on Privacy Enhancing Technologies, 2020.

Shires, James, et al. Gendered Hate Speech, Data Breach and State Overreach. Chatham House, May 2024.

Silk, Jennifer S., et al. "Using a Smartphone App and Clinician Portal to Enhance Brief Cognitive Behavioral Therapy for Childhood Anxiety Disorders." Behavior Therapy, vol. 51, no. 1, Jan. 2020, pp. 69–84.

Singhai, Richa, and Rama Sushil. "An Investigation of Various Security and Privacy Issues in Internet of Things." Materials Today: Proceedings, vol. 80, Jan. 2023, pp. 3393–97.

Skalkos, Andreas, et al. "Users' Privacy Attitudes towards the Use of Behavioral Biometrics Continuous Authentication (BBCA) Technologies: A Protection Motivation Theory Approach." Journal of Cybersecurity and Privacy, vol. 1, no. 4, Dec. 2021, pp. 743–66.

Slawomirski, Luke, et al. Progress on Implementing and Using Electronic Health Record Systems: Developments in OECD Countries as of 2021. OECD, 21 Sept. 2023.

Smalley , Suzanne. "Broker Sold Planned Parenthood Visitor Location Data to Pro-Life Group, Senator Says." The Record, Feb. 2024.

Sobel, Aaron X. "End-Running Warrants: Purchasing Data under the Fourth Amendment and the State Action Problem." Yale Law & Policy Review, vol. 42, 2024 2023, p. 176.

Sobieraj, Sarah. Credible Threat: Attacks Against Women Online and the Future of Democracy . Oxford University Press, 2020.

Sorell, Tom, et al. "Ethical Issues in Computational Pathology." Journal of Medical Ethics, vol. 48, no. 4, Apr. 2022, pp. 278–84.

Stark, Luke, and Jesse Hoey. "The Ethics of Emotion in Artificial Intelligence Systems." Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, Association for Computing Machinery, 2021, pp. 782–93.

Sui, Anna, et al. "Ethical Considerations for the Use of Consumer Wearables in Health Research." Digital Health, vol. 9, Feb. 2023, p. 20552076231153740.

Szlyk, Hannah Selene, et al. "Subgroups of Suicidal Texters Engaging with Crisis Text Line." Psychiatric Services (Washington, D.C.), vol. 71, no. 4, Dec. 2019, p. 319.

Tangari, Gioacchino, et al. Mobile Health and Privacy: Cross Sectional Study. Department of Computing, Macquarie University, Sydney, NSW, Australia, 16 May 2021.

Tangerding, Ellen. Beyond Data Protection: Applying the GDPR to Facial Recognition Technology. 2021. University of Twente.

Tarricone, Rosanna, et al. "Distinguishing Features in the Assessment of mHealth Apps." Expert Review of Pharmacoeconomics & Outcomes Research, vol. 21, no. 4, July 2021, pp. 521–26.

Tertulino, Rodrigo, et al. "Privacy in Electronic Health Records: A Systematic Mapping Study." Journal of Public Health, vol. 32, no. 3, Mar. 2024, pp. 435–54.

Tesink, V., et al. "Neurointerventions in Criminal Justice: On the Scope of the Moral Right to Bodily Integrity." Neuroethics, vol. 16, no. 3, Sept. 2023, p. 26.

Townsend, Kate Goldie. "Defending an Inclusive Right to Genital and Bodily Integrity for Children." International Journal of Impotence Research, vol. 35, no. 1, Feb. 2023, pp. 27–30.

Tran, Quang Nhat, et al. "Biometrics and Privacy-Preservation: How Do They Evolve?" IEEE Open Journal of the Computer Society, vol. 2, 2021, pp. 179–91.

Tsai, Chen Hsi, et al. "Effects of Electronic Health Record Implementation and Barriers to Adoption and Use: A Scoping Review and Qualitative Analysis of the Content." Life, vol. 10, no. 12, Dec. 2020, p. 327.

Turanjanin, Veljko. "Video Surveillance of the Employees between the Right to Privacy and Right to Property after Lopez Ribalda and Others v. Spain." University of Bologna Law Review, vol. 5, 2020, p. 268.

Tyson, Lee Rainie, Cary Funk, Monica Anderson and Alec. "Public More Likely to See Facial Recognition Use by Police as Good, Rather than Bad for Society." Pew Research Center, 17 Mar. 2022.

UK Information Commissioner's Office. Investigation into Data Protection Compliance in the Direct Marketing Data Broking Sector. Oct. 2020.

van de Waerdt, Peter J. "Information Asymmetries: Recognizing the Limits of the GDPR on the Data-Driven Market." Computer Law & Security Review, vol. 38, Sept. 2020, p. 105436.

van der Sloot, Bart, and Yvette Wagensveld. "Deepfakes: Regulatory Challenges for the Synthetic Society." Computer Law & Security Review, vol. 46, Sept. 2022, p. 105716.

Vardanyan, Lusine, et al. "Sciendo." TalTech Journal of European Studies, vol. 12, no. 1, June 2022, pp. 159–85.

Viens, A. M. The Right to Bodily Integrity. Routledge, 2014.

Wahl, Velvet. "How Data Brokers and Phone Apps Are Helping Police Surveil Citizens Without Warrants." Issues in Science and Technology, 6 Jan. 2021.

Wan, Zhiyu, et al. "Sociotechnical Safeguards for Genomic Data Privacy." Nature Reviews Genetics, vol. 23, no. 7, July 2022, pp. 429–45.

Wang, Xiaomei, et al. "Investigating Popular Mental Health Mobile Application Downloads and Activity During the COVID-19 Pandemic." Human Factors: The Journal of the Human Factors and Ergonomics Society, vol. 65, no. 1, Feb. 2023, pp. 50–61.

Westlake, Bryce, and et al. "Developing Automated Methods to Detect and Match Face and Voice Biometrics in Child Sexual Abuse Videos." Trends and Issues in Crime and Criminal Justice, no. 648, Mar. 2022, pp. 1–15.

Williamson, Steven M., and Victor Prybutok. "Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare." Applied Sciences, vol. 14, no. 2, Jan. 2024, p. 675.

Xiang, Chloe. "'He Would Still Be Here': Man Dies by Suicide After Talking with AI Chatbot, Widow Says." VICE, 30 Mar. 2023.

Yao, Rui, et al. "Inequities in Health Care Services Caused by the Adoption of Digital Health Technologies: Scoping Review." Journal of Medical Internet Research, vol. 24, no. 3, Mar. 2022, p. e34144.

Zhang, Dongsong, et al. "Breaking the Data Value-Privacy Paradox in Mobile Mental Health Systems Through User-Centered Privacy Protection: A Web-Based Survey Study." JMIR Mental Health, vol. 8, no. 12, Dec. 2021, p. e31633.

Zhang, Jianhua, et al. "Emotion Recognition Using Multi-Modal Data and Machine Learning Techniques: A Tutorial and Review." Information Fusion, vol. 59, July 2020, pp. 103–26.

Zhang, Shiqing, et al. "Deep Learning-Based Multimodal Emotion Recognition from Audio, Visual, and Text Modalities: A Systematic Review of Recent Advancements and Future Prospects." Expert Systems with Applications, vol. 237, Mar. 2024, p. 121692.

ANNEX 1

Attitudes Toward Bodily Data Collection

Survey 1

Total Respondents: 202

1. Your Age

- 25-34: 87 responses (43.1%)
- 18-24: 53 responses (26.2%)
- 35-44: 43 responses (21.3%)
- 45-54: 12 responses (5.9%)
- 55-64: 4 responses (2.0%)
- 65-74: 3 responses (1.5%)
- 75-84: 0 responses (0%)
- 85-94: 0 responses (0%)
- Under 18: 0 responses (0%)

2. Your Gender

- Male: 101 responses (50.0%)
- Female: 100 responses (49.5%)
- Gender non-conforming: 1 response (0.5%)
- Prefer not to respond: 0 responses (0%)
- Transgender: 0 responses (0%)
- Other: 0 responses (0%)

3. Your Education

- Bachelor's degree: 116 responses (57.4%)
- High school graduate: 48 responses (23.8%)
- Master's degree: 33 responses (16.3%)
- Doctorate: 2 responses (1.0%)
- Other: 3 responses (1.5%)

4. Is your health data stored electronically?

- Some of my health data is stored electronically: 115 responses (56.9%)
- All of my health data is stored electronically: 47 responses (23.3%)
- I am unsure if any of my health data is stored electronically: 20 responses (9.9%)
- None of my health data is stored electronically: 20 responses (9.9%)

5. Who do you think has access to your health data?

- Only the doctors who treat me have access to my health data: 96 responses (47.5%)
- All medical professionals in my country have access to my health data: 68 responses (33.7%)
- I'm unsure who has access to my health data: 23 responses (11.4%)
- Others besides medical professionals may have access to my health data: 15 responses (7.4%)

6. Is your health data stored electronically?

- Some of my health data is stored electronically: 115 responses (56.9%)
- All of my health data is stored electronically: 47 responses (23.3%)
- I am unsure if any of my health data is stored electronically: 20 responses (9.9%)
- None of my health data is stored electronically: 20 responses (9.9%)

7. How concerned are you that others may have access to your health data?

- I'm slightly concerned: 64 responses (31.7%)
- I'm not at all concerned: 49 responses (24.3%)
- I'm fairly concerned: 48 responses (23.8%)
- I'm very concerned: 41 responses (20.3%)

8. Would you consider opting out of any digital health records system if your health data was shared beyond your doctors?

- I might consider opting out, depending on what data is shared and with whom: 113 responses (55.9%)
- Yes, I would definitely consider opting out: 62 responses (30.7%)
- I would never consider opting out just because of data sharing: 27 responses (13.4%)

9. Which of the following sentences do you find acceptable?

- I don't mind if my health data is shared for scientific research, even if I don't benefit directly: 116 responses (57.4%)
- I don't mind if my health data is shared for scientific research that benefits me directly: 101 responses (50.0%)
- I don't mind if my health data is shared for law enforcement purposes: 66 responses (32.7%)
- I don't mind if my health data is shared for financial profit making, and the profit is shared with me directly: 58 responses (28.7%)
- None of the above: 22 responses (10.9%)
- I don't mind if my health data is shared for financial profit making, even if not shared with me: 15 responses (7.4%)

10. Do you feel you have a real opportunity to opt out of using electronic health records systems?

- No, I don't think I could stop using them: 95 responses (47.0%)
- Yes, I believe I could stop using them whenever I wanted: 53 responses (26.2%)
- I'm unsure if I could stop using them: 49 responses (24.3%)
- Not relevant for me: 5 responses (2.5%)

11. Have you ever used a mobile health app?

- Yes, I have used (or currently use) a mobile health app: 154 responses (76.2%)
- No, I have never used a mobile health app: 44 responses (21.8%)
- I'm unsure if I have ever used a mobile health app: 4 responses (2.0%)

12. If you answered yes to the previous question, please specify which of the following apps you have used before.

- Fitness and Exercise Apps: 136 responses (78.2%)
- Diet and Nutrition Apps: 67 responses (38.5%)
- Women's Health Apps: 64 responses (36.8%)
- Sleep Tracking Apps: 60 responses (34.5%)
- Health Monitoring Apps: 44 responses (25.3%)
- Meditation and Mindfulness Apps: 38 responses (21.8%)
- Mental Health and Behavioral Apps: 19 responses (10.9%)
- Substance Abuse Apps: 4 responses (2.3%)
- Other: 9 responses (5.2%)

13. Who do you think has access to the data that you share on mobile health apps?

- Only the service providers have access to the data: 74 responses (36.6%)
- Others besides the service providers may have access: 65 responses (32.2%)
- I'm unsure who has access to the data: 62 responses (30.7%)

14. How concerned are you that others may have access to the data you share on mobile health apps?

- I'm slightly concerned: 73 responses (36.1%)
- I'm fairly concerned: 58 responses (28.7%)
- I'm very concerned: 37 responses (18.3%)

- I'm not at all concerned: 34 responses (16.8%)

15. Would you consider opting out of using a mobile health app if you learned that your data was shared with others beyond the service providers?

- I might consider opting out, depending on which app and what data is shared: 86 responses (42.6%)
- Yes, I would definitely consider opting out: 84 responses (41.6%)
- No, I would never consider opting out just because of data sharing: 32 responses (15.8%)

16. Which of the following apps would you consider opting out of if you learned that they share your data with others?

- Fitness and exercise apps: 71 responses (35.1%)
- Mental health and behavioral apps: 67 responses (33.2%)
- Women's health apps: 67 responses (33.2%)
- Health monitoring apps: 63 responses (31.2%)
- Sleep tracking apps: 63 responses (31.2%)
- Diet and nutrition apps: 57 responses (28.2%)
- Substance abuse apps: 43 responses (21.3%)
- Meditation and mindfulness apps: 33 responses (16.3%)
- None of the above: 27 responses (13.4%)

17. Do you feel like you have a real opportunity to opt out of mobile health apps?

- Yes, I believe I could stop using them whenever I wanted: 114 responses (56.4%)
- In certain cases, I could stop using them; in other cases, probably not: 49 responses (24.3%)
- No, I don't think I could stop using them even if I wanted to: 26 responses (12.9%)
- I'm unsure if I could stop using them: 13 responses (6.4%)

18. Which of the following sentences do you find acceptable?

- I don't mind if my biometric data is shared for scientific research that benefits me directly: 120 responses (59.4%)
- I don't mind if my biometric data is shared for scientific research, even if the results may not benefit me directly: 97 responses (48.0%)
- I don't mind if my biometric data is shared for law enforcement purposes: 64 responses (31.7%)
- I don't mind if my biometric data is shared for financial profit making and the profit is shared with me directly: 60 responses (29.7%)
- None of the above: 26 responses (12.9%)
- I don't mind if my biometric data is shared for financial profit making, even if that profit is not shared with me: 10 responses (5.0%)

19. Have you ever been subject to biometric data collection?

- Yes, I have been subject to biometric data collection before: 148 responses (73.6%)
- No, I have never been subject to biometric data collection: 35 responses (17.4%)
- I'm unsure/unaware if I've ever been subject to biometric data collection: 18 responses (9.0%)

20. If you answered yes to the previous question, please specify which biometric data collection technique you have been subject to.

- Fingerprint recognition: 139 responses (83.2%)
- Face/facial recognition: 138 responses (82.6%)
- Voice recognition: 53 responses (31.7%)
- Emotion (or affect) recognition: 14 responses (8.4%)
- Iris and/or retina recognition: 13 responses (7.8%)
- Keystrokes recognition (typing styles): 11 responses (6.6%)
- Palm vein recognition: 10 responses (6.0%)
- Gait recognition (body shape and walking styles): 7 responses (4.2%)
- Other: 3 responses (1.8%)

21. Who do you think has access to your biometric data?

- Only the organizations who collect my biometric information can access that data: 106 responses (52.5%)
- I'm unsure who has access to my biometric data: 52 responses (25.7%)
- Others besides the organizations who collect my biometric information may also access that data: 44 responses (21.8%)

22. How concerned are you that others may have access to your biometric data besides the organizations collecting it?

- I'm slightly concerned: 66 responses (32.7%)
- I'm very concerned: 64 responses (31.7%)
- I'm fairly concerned: 45 responses (22.3%)
- I'm not at all concerned: 27 responses (13.4%)

23. Would you consider opting out of any biometric data collection method if you learned that your biometric information was shared beyond the organizations collecting the data?

- Yes, I would definitely consider opting out: 99 responses (49.0%)
- I might consider opting out, depending on what data is shared and with whom: 81 responses (40.1%)
- I would never consider opting out, even if my data was shared: 22 responses (10.9%)

24. Do you feel like you have a real opportunity to opt out of biometric data collection?

- In certain cases, I think I could opt out; in other cases, probably not: 68 responses (33.7%)
- Yes, I believe I could opt out whenever I wanted to: 68 responses (33.7%)
- No, I don't think I could opt out of any of these data collection methods, even if I wanted to: 43 responses (21.3%)
- I'm unsure if I could opt out of biometric data collection: 23 responses (11.4%)

25. Which of the following sentences do you find acceptable regarding your biometric data?

- I don't mind if my biometric data is shared for scientific research that benefits me directly: 96 responses (47.5%)
- I don't mind if my biometric data is shared for law enforcement purposes: 71 responses (35.1%)
- I don't mind if my biometric data is shared for scientific research, even if the results may not benefit me directly: 63 responses (31.2%)
- I don't mind if my biometric data is shared for financial profit making and the profit is shared with me directly: 54 responses (26.7%)
- None of the above: 47 responses (23.3%)
- I don't mind if my biometric data is shared for financial profit making, even if that profit is not shared with me: 13 responses (6.4%)

ANNEX 2

Attitudes Toward Data Sharing in Specific Scenarios

Survey 2

1. **Cyber Attack on Health Data:**

- Question: "You hear about a recent cyber attack where hackers accessed sensitive health data from a hospital and demanded a ransom for its release. What are the first three words that come to your mind about this?"
- Common Words: Anger, fear, distrust
- Sentiment Score: Predominantly negative, reflecting significant concern about security and privacy, with many articulating feelings of vulnerability.

2. **Leaked Health Data Impacting Insurance Costs:**

- Question: "You learn that leaked health data can negatively impact insurance costs, resulting in increased premiums for individuals with existing medical conditions whose information was compromised during a data breach. What are the first three words that come to your mind about this?"

- Common Words: Invasion of privacy, unacceptable, dangerous
- Sentiment Score: Predominantly negative, demonstrating heightened sensitivities regarding the financial implications of data breaches.

3. **Fitness App Data Shared with Third-Party Firms:**
- Question: "You learn that the fitness tracking app you use has been sharing your activity levels and workout data with a third-party marketing firm without your knowledge. What are the first three words that come to your mind about this?"
- Common Words: Betrayal, manipulation, exploitation
- Sentiment Score: Negative, with 54.5% of respondents expressing concern about their information being used without their consent.

4. **Reproductive Health App Sharing Sensitive Information:**
- Question: "You discover that the reproductive health app you use for tracking menstrual cycles has shared sensitive information with outside companies for research and product development without your explicit consent. What are the first three words that come to your mind about this?"
- Common Words: Betrayal, anger, violation
- Sentiment Score: Predominantly negative, with 45.9% of participants expressing concern about unauthorized data sharing.

5. **Mental Health Data Shared with Researchers:**
- Question: "You learn that the mental health app you've been using has shared data about your moods and coping strategies with researchers studying mental health trends. What are the first three words that come to your mind about this?"
- Common Words: Untrustworthy, invasive, manipulative
- Sentiment Score: Negative, with 53.1% of respondents expressing unease about their anonymized data being utilized without explicit consent.

6. **Law Enforcement Accessing Health Records:**
- Question: "You learn that your electronic health records have been accessed by law enforcement as part of an investigation into a series of fraud cases. What are the first three words that come to your mind about this?"
- Common Words: Anger, fear, insecurity
- Sentiment Score: Predominantly negative, with 38.4% of respondents being very concerned about this unauthorized access.

7. **Biometric Data Shared with Research Institute:**
- Question: "You learn that your biometric data, such as your fingerprint and facial recognition information collected by your bank for security purposes, will be shared with a research institute studying fraud prevention measures. What are the first three words that come to your mind about this?"
- Common Words: Very concerned, betrayal, violation
- Sentiment Score: Strongly negative, with 61.1% of participants expressing concern about sharing biometric data without their explicit consent.

8. **Facial Recognition Data for Airport Safety:**
- Question: "You learn that your facial recognition scans captured at an airport are being shared with researchers studying the effectiveness of biometric security measures. What are the first three words that come to your mind about this?"
- Common Words: Very concerned, invasive, unsafe
- Sentiment Score: Predominantly negative, with 48% of respondents very concerned about privacy violations.

9. **Biometric Data Sold for Commercial Use:**
- Question: "You find out that your fingerprint scans collected by a financial institution are being sold to a tech company developing new biometric authentication tools. What are the first three words that come to your mind about this?"
- Common Words: Very concerned, unfair, exploitation
- Sentiment Score: Strongly negative, with 47.5% expressing concern about their data being used for profit without their consent.

10. **Iris Scans Sold Without Compensation:**
- Question: "You learn that your iris scans, captured during a security check at work, have been sold to a security solutions company for the development of new monitoring solutions. What are the first three words that come to your mind about this?"
- Common Words: Very concerned, unfair, unethical
- Sentiment Score: Strongly negative, with 61.6% of respondents expressing outrage about their