Chapter 17
The Ethics of Privacy in Research and Design: Principles, Practices, and Potential

Lorraine Kisselburgh and Jonathan Beever

Abstract The contexts of sociotechnical privacy have evolved significantly in 50 years, with correlate shifts in the norms, values, and ethical concerns in research and design. We examine these eras of privacy from an ethics perspective, arguing that as contexts expand from the individual, to internet, interdependence, intelligences, and artificiality, they also reframe the audience or stakeholder roles present and broaden the field of ethical concerns. We discuss these ethical issues and introduce a principlist framework to guide ethical decision-making, articulating a strategy by which principles are reflexively applied in the decision-making process, informed by the rich interface of epistemic and ethical values. Next, we discuss specific challenges to privacy presented by emerging technologies such as biometric identification systems, autonomous vehicles, predictive algorithms, deepfake technologies, and public health surveillance and examine these challenges around five ethical principles: *autonomy*, *justice*, *non-maleficence*, *beneficence*, and *explicability*. Finally, we connect the theoretical and applied to the practical to briefly identify law, regulation, and soft law resources—including technical standards, codes of conduct, curricular programs, and statements of principles—that can provide actionable guidance and rules for professional conduct and technological development, codifying the reasoning outcomes of ethics.

L. Kisselburgh (✉)
Purdue University, Center for Education and Research in Information Security, Burton Morgan Center for Entrepreneurship, West Lafayette, IN, USA
e-mail: lorraine@purdue.edu

J. Beever
Department of Philosophy, Center for Ethics, University of Central Florida, Orlando, FL, USA
e-mail: jonathan.beever@ucf.edu

B. P. Knijnenburg et al. (eds.), *Modern Socio-Technical Perspectives on Privacy*,
https://doi.org/10.1007/978-3-030-82786-1_17

17.1 Introduction

Privacy is an ethical issue. Almost every chapter in this volume takes on these issues to some degree, whether in the broader context of cultural norms (Chap. 5), the professional context of codes of ethics (e.g., Chap. 6), as cultural values (Chap. 12), or as an implicit good in the discussions of privacy enhancements or violations (Chap. 8). This chapter develops a typology of the ethics of privacy, emphasizing the roles and responsibilities of the researcher. We draw a parallel between the ethics of design and the landscape of privacy research, arguing that a structured reflexive approach to ethical decision-making is required in the complex and changing landscape of contemporary privacy practices, problems, and policies.

To begin, we take a historical approach to typologizing the ethics of designing technologies for privacy. In this first section, we outline key terms as a means of grounding our discussion on a carefully defined sense of ethics and understanding of the moral agents and patients involved. The next section examines the eras of privacy research from an ethics perspective, arguing that ethical values within privacy discussions have and are again shifting, reemphasizing the need to continued development of ethics literacy in this area. We articulate a strategy of ethical decision-making by which decision-makers can thoughtfully adjudicate among conflicting values within privacy debates. That decision-making strategy can help us reframe contemporary privacy challenges, the target of our fourth section, by drawing attention to changes in the ethical landscape. Next, we outline emerging ethical challenges, arguing that historical/traditional conceptualizations of privacy limit our ability to consider privacy issues of contemporary technologies in the AI era and beyond. Finally, we consider some implications for an ethically literate perspective on privacy practice and policy.

17.2 Eras of Privacy Ethics

We begin with an outline of eras of privacy research from an ethics perspective, arguing that the ethical issues around privacy discussions have and are again shifting, reemphasizing the need to continued development of ethics literacy in this area.

17.2.1 Research Ethics and Emerging Technologies

In the context of research and design, ethics is concerned with the moral issues that arise during or as a result of research activities, as well as the ethical conduct of researchers. Discussions of ethics are scaffolded from issues within research practices (“research ethics” or “responsible conduct of research”) and the

societal and environmental implications of that research ("broader impacts"). This scaffolding of ethics is historically driven: a result of notorious unethical research practices in the early twentieth century.

Notably, the revelation of bioethical scandals such as the Guatemala STD studies and the cultivation and dissemination of the HeLa cell line in the United States led to the realization that clear measures were needed for the ethical governance of research to ensure that people, animals, and environments are not unduly harmed in research. Yet when US physicians experimented on Guatemalan prisoners of color, women, and children without consent [1], the ethical concern was not *merely* about the physical harms involved. Similarly, the use of Henrietta Lacks' genetic material without her consent was not *merely* about disrespecting her autonomy (see [2, 3]). Importantly, these and other cases of unethical research involved an ecosystem of ethical concern based on what we owe each other. What has become known as *bioethical principlism* [4] defines four key universally applicable principles: non-maleficence (avoiding harms), beneficence (doing good), justice, and respect for autonomy. In the context of research, all four principles are in play together outlining the complex landscape of rights and responsibilities. Thus, the harms done to research subjects in Guatemala or to Henrietta Lacks and her family posed ethical challenges to individuals' rights, broadly construed, and can be seen through the lens of privacy.

As bioethics has evolved in the US context, its principles have come to mark out a broad ethical territory that is not only about the research practice itself (say, extracting biological samples from human subjects in the clinic) but also about the design of processes that lead up to, frame, and fall out from those practices. Emphasis on the processes of design draws attention to the *reflexivity* between normative principles and the context in which they are applied (see [5]). A *reflexive*[1] principlism [6] is analogous to the design process in that they both rely on a cyclical application and analysis of principles considered through constraints of particular stakeholders or audience and specifics of the real-world context.

Stakeholders in ethics play roles either (or both) as moral agents or (or and) moral patients. Moral agents have the capacity and therefore the responsibility to act ethically, and moral patients have moral rights based on some capacity or characteristic they have. As bioethical principlism has evolved alongside the technologies with which it interfaces, those relationships among agents and patients have become more diverse and more complicated. Theoretical and practical concerns about physical harms became the impetus for the wider net of research ethics cast to focusing broadly on the implications of technology practices on lived experience. Contemporary research ethics (see [7]) marks out the points of intersections among the human interests and technological influences. But as the technology landscape continues to evolve and integrate into the experiences of living entities (human

[1] We take *reflexion* to be an unconscious habituated response, whereas *reflection* is a conscious, deliberate process of thinking about what one is doing. Both are necessary conditions of robust ethical decision-making.

and nonhuman alike), the ethics of research and design also continues to evolve. Each part of research ethics continues to get both more complicated and more interconnected as emerging technologies break down the spaces between them. As an example, consider the collection and sharing of human genetic information, which puts individual and public health considerations up against individual rights and privacy concerns. Issues like these are the direct result of the information technologies, economies, and ecosystems that have so rapidly evolved since the mid-twentieth century. With this evolution, careful ethical distinctions—say, between physical, dignitary (psychological or emotional), and informational harms—play increasingly important roles in conversations about the collection, curation, and use of information.

17.2.2 Changing Contexts of Concern

The terrain of research ethics drives ethical concern about privacy not only historically but also in the contemporary context. Yet what is ethically salient about privacy changes with the social and technological context [8]. We argue that the context under which privacy has been considered has shifted in the past several decades as a direct result of the influences of information technologies. We identify five privacy paradigms that have shifted the ethical salience of privacy research from merely a focus on the human individual through a future of privacy discourses among artificial systems apart from human experiences (Fig. 17.1). These paradigms intersect in robust ways; yet it is helpful to think about them as expansions to more clearly engage relevant privacy practices and policies.

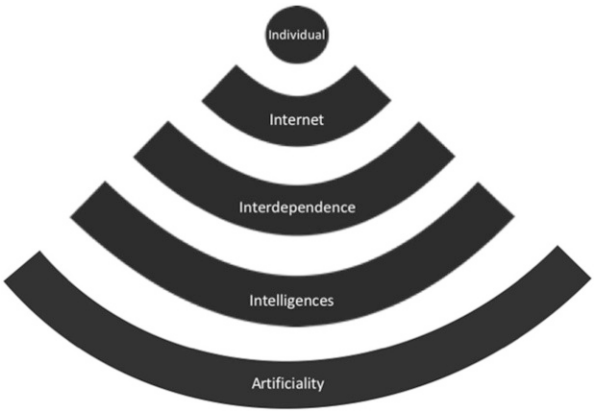

Fig. 17.1 Expansions of privacy contexts

17.2.2.1 Privacy 1.0

In what we might call *Privacy 1.0*, ethical attention was focused on risks of dignitary harms[2] to the individual citizen. In the US context, ethical concerns about privacy have a long history (see [1]). The ethical focus of Privacy 1.0 was codified in legal precedence in what has become known as the "Katz test," proposed by US Supreme Court Justice Harlan in his concurring opinion in the 1967 Katz v. United States case. There, Harlan proposed a two-part test of privacy: that "a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable" [9]. This legal ruling solidified an ongoing social debate about the rights of citizens to be legally (and ethically) protected against *unreasonable* breaches of their privacy. For example, if a citizen has a conversation in her home with doors and shutters closed, she has evidenced an expectation of privacy that is arguably reasonable—even if someone else can overhear that conversation from the sidewalk outside. Yet if the doors and shutters are thrown wide, there is no such evidence and, therefore, arguably less legal protection for her privacy. So while it had been seen as reasonable for conversations taking place within one's home to be protected as private, it was at that time much less clear how far that protection extended or what constituted *reasonableness*. For our purposes, this legal ruling is less important than the core framing question to which it gives voice: namely, what kinds of information are protected as private and in what contexts?

17.2.2.2 Privacy 2.0

As information technologies quickly expanded in the mid twentieth century, ethical concerns about privacy expanded in reaction. The rise of Internet technologies brought into stark relief what we will call *Privacy 2.0*, expanding concerns about dignitary harms from a local to a global level. The Privacy Act of 1974 [10] in the United States codified privacy concerns in the emerging information age, at least in the context of information collected, maintained, used, and disseminated by federal agencies. That Act mandated limits on transmission of information about individuals, offering baseline protections for information privacy. Responding to tensions among ethical values related to economy, access, and privacy in the emerging information age, legislation like the Privacy Act pushed the focus of the ethics of privacy from the individual to the Internet, expanding the scope of privacy concerns. Importantly, this shift in focus pushed back the locus of ethical inquiry from a view of the isolated individual agent and toward the individual's information.

Information philosopher Luciano Floridi, in his 2013 *Ethics of Information*, argued for an informational interpretation of the self and, therefore, a focus on

[2] Dignitary harms differ from physical harms in that they are not bodily but psychological or, in our current context, informational.

informational privacy. In his view, privacy researchers distinguish among four types: physical, mental, decisional, and informational ([11], p. 230). Floridi offers the example of a typical human moral agent [12], Alice, to help make these distinctions. Alice's **physical** privacy is contingent on constraints on her embodied experience, including sensory or mobility interference. When we get ready for a Zoom meeting, we might each demand this kind of physical privacy in asking to be allowed to dress or frame the scene offline rather than sitting in front of the camera. But privacy for Floridi's Alice also includes **mental** privacy, or freedom from psychological interferences to her mind and mental states. While an individual preparing for a Zoom meeting might request physical privacy, they may have no similar desires concerning mental privacy; indeed, perhaps they are on the phone with a colleague talking about structure for the meeting. Alongside physical and mental privacy, Alice is also owed or at least has the capacity for **decisional** privacy. Alice's decisional privacy requires autonomous decision-making, free from interference by others. Finally, Floridi circles back around to the idea of **informational** privacy, or freedom from restrictions on facts—what Floridi calls "epistemic interference" (p. 230). These four categories define the horizon of Alice's privacy landscape, acting as the parameters for discussions about what we owe her, morally. Now, Floridi's broader argument concerning informational privacy is that what he calls "old" information, and computing technologies (ICTs) reduce this kind of privacy, whereas new ICTs can either decrease or *increase* informational privacy. Floridi notes that "solutions to the problem of protecting informational privacy can be not only self-regulatory and legislative but also technological, not least because information privacy infringements can more easily be identified and redressed, also thanks to digital ICTs" (p. 236). While he argues against our reading this claim as an "idyllic scenario" (p. 236) of technological optimism, the idea that increases in quality (scope), quantity (scale), and speed[3] of informational technologies will *equitably* increase opportunities for benefits and harms is difficult to evidence.

This account is important in that it addresses multiple aspects of the ethics of privacy. First, Floridi argues for an expansion of the *scope* of privacy concerns, from individual to information through Internet technologies. Second, Floridi argues for a change in the *scale* of privacy concerns, suggesting that information technologies, *ceteris paribus*, are value neutral in that they can either decrease or increase privacy thanks to the scale, scope, and speed of information exchange they enable. Floridi's ontological account of ICTs reframes traditional discussions of privacy ethics and policy by baselining out both human individuals and computational technologies as the same kind of entities, namely, informational entities. Imagine here the difference between slander in a local newspaper in the 1950s compared to slander on global

[3] There are several similar descriptions of digital data. Analyst Doug Laney introduced "three V's" of data – volume, variety, and velocity – in a 2001 report [13]. A 2015 National Institute of Standards and Technology (NIST) report defined a six-part parallel description of data that included validity, velocity, veracity, vertical scaling, volatility, and volume [14].

social media in the early 2000s. Privacy concerns are broader and potentially more significant under the 2.0 paradigm than under its 1.0 predecessor.

17.2.2.3 Privacy 3.0

The changes in scope, scale, and speed of information transfer enabled by contemporary information technologies have pushed privacy concerns from extensions of my information to networks of my information, or from internet to *interdependence*. Interdependence, or the networking relations of information that constitute each individual, shifts the burden of privacy further from the isolated individual (whether local or global) to the network of information to which that individual is connected and through which that individual is constituted [15]. This shift from Privacy 2.0 to Privacy 3.0 is ontologically uncomfortable, since many of us are culturally habituated into a worldview that privileges the view that the individual somehow stands alone. Floridi's Alice stands for just such a traditional individual moral agent from Privacy 2.0. Yet extensions of information through both digital and analog environments challenge this worldview.

In a recent book looking at interdependence through the lens of film, Beever argues that another Alice—this one from the science fiction film series *Resident Evil* [16]—represents this relational paradigm of privacy concerns. Here, Alice exists as a cloned instance of some original Alice and is constituted as a complex amalgam of technologies, an inherited set of information, and unique lived experiences and interpersonal connections. Alice is not Alice *except* for these relationships: indeed, in this fictional context, there is nothing essential to her character about her physical form or, even, her genetic information. This film series is compelling because it complicates and extends the realities of interdependence to show us moral threat in the digital extensions of the self: "interdependence with other information flows like the virus is interdependent with the host" (p. 186). We need not stretch to the science fictional to understand this paradigm shift of privacy concerns. Consider, as a real-world example, the myriad roles that genetic information plays in our understanding of who we are and how we relate. A single sample can share with others information about our relational selves that we did not yet know. Similarly, algorithms that drive our digital platforms deny or define our choice of relations (whether social media streams, the Internet access, or shopping choices), defining who we are by what we know and to whom we have access. In this Privacy 3.0 paradigm, informational interdependence governs new responses to our core question: "what kinds of information are protected as private and in what contexts?" (e.g., [17–19]). Committed to an information ontology but also an epistemic and ethical position that our relations constitute what we know and what we value, the response to this question is now broader and more complicated.

17.2.2.4 Privacy 4.0

Across privacy paradigms, the onus of ethics has been on the definition and defense of human individual rights regarding their information. Changes to the technological landscape and, in turn, the speed, scope, and scale of digital information were the predominant focus, while the moral target remained the same. In what we call Privacy 4.0, it is the target of ethical inquiry that changes. Here, artificial intelligence systems present a potentially novel kind of ethical agent: a nonhuman nonorganic agent that conflates the categories of the previous privacy paradigms. AI systems thread together individual agency, Internet big data technologies, and interdependence. In so doing, they offer a new space of ethical discourse between human agents and these nonhuman artificial agents. Ongoing efforts to define what constitutes "ethical" AI have led to a convergence around five ethical principles: transparency, justice, non-maleficence, responsibility, and privacy [20]. There are clear parallels here between this set of normative principles and the principles of bioethics; justice and non-maleficence remain key ethical principles. Yet in the place of autonomy and beneficence stand transparency, responsibility, and privacy, emphasizing the focus on information structures, use, and representation. In Privacy 4.0, human individuals and AI systems are combined together as two types of information systems. Human individuals play roles in this ethical landscape not only as users (moral patients) but as collaborating moral agents, designers, and developers of artificial information systems. Developing reflexivity in the analysis and application of these principles is just as important as it is within the Privacy 1.0 paradigm. But reflexivity takes on new meaning as an encoded ability of complex information systems.

17.2.2.5 Privacy 5.0

As we look toward the future of the ethics of privacy, we envision a Privacy 5.0 paradigm in which the reflexive process of ethical decision-making takes place between two artificial information systems. In this paradigm, the human agent is wholly excluded, having participated (perhaps) as the designer of a now wholly autonomous artificial agent. While this paradigm is still largely the stuff of science fiction, it is visible on the horizon of our technological development. Thinking about the value of privacy as something understood and negotiated outside of the participation and direct guidance of human moral agents enables us to think proactively about practices and policies around privacy now.

The five paradigms of privacy laid out in this section reframe the complex stakeholder or audience roles present in an increasingly complex information economy. They serve as a heuristic by which to assess ethical practices around privacy, like the practice of informed consent, which may apply in one paradigm but seem outmoded in another. The intersections among paradigms create new research contexts, new social interactions, and new uncertainty that can lead us to renegotiations of legal and regulatory frameworks related to privacy.

17.3 Ethical Decision-Making and Key Issues

In the previous section, we argued that changing paradigms of privacy, enabled by continued development of information technologies, challenge the roles and natures of stakeholders. These challenges reshape the ethical terrain of privacy concerns, adding complexity to analyses of what or whom matters morally and why. In this section, we turn from the theoretical and conceptual concerns to the practical, asking "How do the changing paradigms of privacy challenge our models of ethical decision-making?"

Models of ethical decision-making (EDM) emphasize the procedure of reasoning through complex ethical issues, taking into account not only philosophical concerns about values and value conflicts but also the epistemic or factual context in which those value relations play out (see [21] for a review). Generally speaking, ethical decision-making describes a series of steps to be taken, often in cyclical series, until a decision is reached:

1. Identify the problem.
2. Review the facts.
3. Identify the values at stake.
4. Identify the relevant ethical guidelines (codes or theories).
5. Enumerate consequences, outcomes given the context.
6. Decide on a best course of action.

Ethical decision-making is a dynamic, iterative process that starts with developing ethics sensitivity, or the ability to see a problem as an ethical problem in the first place and to judge its intensity ([22], p. 159). An ethical issue is not identified or evaluated in a vacuum, so the problem is always grounded in epistemic constraints (the *facts*) and assessed through utilization of the tools of normative ethics to get at values and their conflicts (the *values*). The values landscape is informed by normative theories, or structured approaches to how, why, and under what circumstances values apply. Contemporary approaches to EDM often take a pluralistic approach, relying not on a single normative approach (like *either* utilitarianism *or* deontology) but on their fit given the epistemic and ethical context (see [23]).

The reasoning process is not algorithmic but a part of this richly dynamic EDM process, with a goal of producing a pragmatic, context-informed decision. The iterative nature of EDM is itself pragmatic in the same way as is the design process: both recognize that changing constraints or actualization of outcomes might shift the parameters of the decision. *Good* ethical decision-making, then, is the result of practice, or developing the right habits and experiences to work through the process reflexively.

Complexity in ethical decision-making is clearly seen when applied to questions of privacy. For example, should someone submit a cheek swab to a genetic information corporation? With limited ethical sensitivity, we might not be attuned to the ethical tensions between access to, say, some details about our ancestry and

the ways in which my information will be digitized and monetized. But without a robust understanding of relevant business models, digital information policies and practices, and social context, worrying about our data is ungrounded.

Ethical decision-making is a process of application of the principlism we outlined in the last section. Indeed, principlism does not offer a decision-making process but, instead, "an analytical framework of general norms . . . that form a suitable starting point for reflection on moral problems . . ." ([4], p. 13).[4] Principlism enters the EDM process directly at steps three and four, where adjudication among values meets the context in which it applies. Ethical principlists have argued that the process of specification and balancing principles in context moves principlism from theory to practice (see [5]). Yet EDM is guided by ethical principles; indeed, without them, it would be simple decision-making. Also essential to the process is the targets, or stakeholders. Ethical decision-making both applies *to* moral patients (those individuals who matter, morally) and is applied *by* moral agents (those individuals capable of making ethical decisions). We turn next to this relationship between patients and agents in the context of privacy paradigms, distinguishing between modes of ethics reception and ethics transmission.

17.3.1 Principles and Patients: Reception

The four ethical principles of principlism offer a pluralistic approach to the major normative theories in ethics: beneficence and non-maleficence considering consequences or utility of actions, and justice and autonomy worrying about rights and duties of individuals who matter morally, otherwise known as *moral patients*. Too much of ethics of technology work has focused too heavily on consequences. For example, much of the early discussion around the ethics of self-driving cars has drawn on trolley problem variants to consider strategies for dealing with the consequences of decisions by the system: does it protect the driver, one or another type of pedestrian, the manufacturer's reputation, etc. [24]? That focus is important here, since it empowers ethical decision-making to focus on consequences for moral patients. But it is also insufficient as it leaves out broader questions of rights.

Privacy concerns are concerns about both the ethical consequences of actions and the rights of the user, stakeholder, or audience. Breaches of privacy can lead to significant dignitary harms by failing to acknowledge or uphold the right to privacy of the individual. Consider the example of Internet of Things (IoT) devices in the home. When my IOT devices are listening to my choices and using those for marketing purposes, they present me with tension between two competing ethical values: access and privacy. I might value access at the expense of privacy and, say, not even read the disclosures that come with my devices. Or I might value privacy

[4] The authors add, "... in biomedical ethics," unnecessarily, on our view, since we argue principlism applies to any discipline or professional that utilizes a version of the design process.

at the expense of access and not allow IOT devices access to my information in the first place. There is less risk to physical Privacy (think Privacy 1.0) than there is risk to informational privacy (think Privacy 2.0+). Thus, privacy concerns are different ethical concerns than other technology-related ethical issues precisely because they are informational.

Without understanding both why a moral patient would value privacy and what consequences breaches of privacy might have, we moral agents cannot effectively evaluate the moral salience of those devices. A recent article in Canadian Bar Association's *National* magazine has received considerable attention for asking the question: "should we recognize privacy as a human right?" [25]. Its author notes that while Canada has introduced legislation to strengthen its consumer privacy protections, it does not "explicitly recognize privacy as a human right, nor does or [sic] give precedence to privacy rights over commercial considerations" (ibid). Whether privacy should be taken up as a basic human right is contingent on its moral salience which, again, is contingent on our understanding of the complex epistemic and ethical contexts in which it functions.

We can think of these ethical tensions and practical responses as on the *receiving end* of ethical discourse. That is, as we focus on the consequences of privacy application or breach, we evaluate the moral patient receiving benefits or harms or negotiating impacts to fairness or free action.

17.3.2 Action and Agents: Transmission

On the *sending end* of ethical discourse, the discussion shifts from outcomes to agency and intention, or from conduct to character. Ethical concern lies not with the moral patient but instead with the moral agent. What responsibilities or duties does the moral agent have vis-à-vis privacy? Questions of character are the focus of *virtue ethics*, one of the oldest normative theories in western philosophical ethics. Reflexive principlism does not emphasize virtue ethics within its pluralism. Rather, one of its designers, Tom Beauchamp, argued that virtue ethics and principlism were complementary [26]. He argues that "virtue theory is of the highest importance in a health-care context because a morally good person with the right motives is more likely to discern what should be done, to be motivated to do it, and to do it" (pp. 194–5). In the same way we have proposed to extend biomedical principlism to other design-based disciplines, we likewise extend Beauchamp's argument. We agree that in design-based contexts, "morally good" agents are more likely to engage in ethical decision-making and act rightly.

A principles-based approach to EDM offers an ethical orientation to real-world problems but is incomplete without complementarity from a theory of the virtue of the agents involved. Virtue ethics complements principlism in the EDM process specifically because privacy stakeholders propose to treat human participants and artificial information systems as collaborating moral agents. Thus, we must be able to evaluate both the receiving and the transmission ends of ethical action.

To situate the idea of the sending end of ethics in a practical context, consider the ethics of digital breast imaging. Medical science continues to prove the benefits of early-detection mammography. Yet there are risks involved, as with any medical procedure, including a low risk of psychological stress from false positives, the even lower risk of physical harm from the mechanical procedure itself, or privacy risks from failure to keep confidential the resulting images. But federal regulations like the US Health Insurance Portability and Accountability Act [27] might offer protection and legal recourse against these types of physical harms, so from individual and public health perspectives, the benefits of digital breast imaging significantly outweigh its harms.

Yet this analysis is over-simplified given the complexity of privacy paradigms. The contemporary landscape of breast imaging involves not traditional mammography but digitally stored and transferred AI-analyzed medical imaging. AI systems continue to be developed for screening, diagnosis, risk calculation, clinical decision support, and management planning [28]. While these advances in health-care technology show promise [29], they also promise peril. The ways that AI systems handle privacy concerns are twofold: First, value priorities are encoded by human designers into the algorithms used by the system; then the system prioritizes that set of values in its learning processes. Thus, privacy concerns here involve potentially *two types* of moral agents on the sending end of ethics: the human and the artificial. While current AI systems are limited in this moral capacity [30], the future of AI development leaves open that Privacy 5.0 door.[5] Privacy policies and practices will have to adapt in order to continue to uphold privacy as a fundamental right [31].

17.3.3 Privacy's Network and Hub

The reception (involving moral patients) and transmission (involving moral agents) of privacy ethics through the process of ethical decision-making rely on the ongoing specification and balancing of principles. The speed and scale of technology development challenge the goal of cultivating ethical reflexivity: habituation is hard under conditions of change. Thus, ethical decision-making around privacy-in-design will continue to demand epistemic and ethical vigilance.

If we think of the hub of privacy ethics as the ethical principles and epistemic value contexts, then its network is the landscape of specified ethical issues (see Table 17.1). The importance of the principlist framework is that it provides a shared normative framework across the various disciplines, professions, and governance bodies with a stake in discussions of privacy. The work of balancing and specifying principles allows several perspectives on what is most ethically salient about, say,

[5] We note that we have offered several medical ethics examples in our discussion so far because those carry significant ethical salience. But our analysis applies broadly to many case contexts involving information systems and value relations with which they interact.

Table 17.1 Ethical principles, cases, human rights, and key privacy concepts

Ethical principle	Autonomy	Justice	Non-maleficence	Beneficence	Explicability
Dimensions	Respect for human dignity, human determination, and oversight; respect for person; right to be left alone; freedom from intrusion	Fairness, equality (non-bias), diversity	Prevention of harm; protection of vulnerable populations; robust, safe, secure	Societal well-being, social impact	Transparency, intelligibility, accountability, traceability
Use cases	Autonomous vehicles, facial recognition, biometric databases	Algorithmic bias; social credit scoring; robot judges, predictive policing	Deepfakes, disinformation, ethnic surveillance	Privacy by design, ICT4All, AI4Good, pandemic health, sustainability	AI black boxing, predictive algorithms
Key privacy concepts	Agency, consent, confidentiality; freedom from intrusion	Due process, right to access, correct, redress	Security; minimization of data, use, and purpose	Data protection	Access, audit, accountability, transparency
Universal Declaration of Human Rights	Respect for human dignity, freedom from arbitrary interference, protection of identity, freedom to make decisions	Non-discrimination, liberty, right to justice, equality, right to remedy	Freedom from arbitrary detention, freedom from arbitrary interference	Responsibility to community	Rights to access public documents, rights to public goods

the principle of non-maleficence in any particular context. By requiring ongoing ethical discourse, principlism empowers collaborative decision-making.

But as privacy paradigms advance, privacy as a value appears more and more in conflict with other values, including access, interaction, and engagement with other information systems. Beyond risk and harm analyses, beyond questions of consent, and beyond aged questions of agency and autonomy, the concern is that *privacy is dead*. In making this claim, we channel Friedrich Nietzsche who, in the late nineteenth century, made a similar claim about God [32]. Nietzsche's acerbic claim was that what we had taken to be God had become, in his view, unbelievable. The death of that particular metaphysical belief was the result of human scientific and technological advancement, which brought into question the religious metaphysic that had guided much of western society. Without that grounding in a view of God, Nietzsche worried that what was left was nothingness: *a void of meaning*. When we say that privacy is dead, we suggest that what we have taken to be privacy no longer has meaning, thanks to tremendous changes in the technology landscape. Privacy is unbelievable because human existence in current (and future) privacy paradigms is defined by how we manage, not restrict, access. And so privacy, like God for Nietzsche, has become a mere simulacrum of doctrine and concept. Thinking about privacy as a practical possibility for which societies can legislate protections is now naive. Contemporary work on privacy continues to reshape the concept as an important if complicated value in the human experience.

17.4 Reframing Privacy Ethics: Emerging Ethical Challenges

Recognizing the broadened social and technological contexts that have shifted the ethical salience of privacy concerns from the individual to interdependent networks and to futures of artificiality and the decision-making frameworks that can assist us in asking what or whom matters morally and why, we turn now to discuss specific emerging ethical challenges pushing us to reconceptualize privacy ethics. We anchor this reconception of privacy in a foundation of universal human rights, recognized throughout the world with the establishment of the Universal Declaration of Human Rights [33] and encoded in international law and treaties. These rights are legally enforceable and provide clear consequences for violations. They include specific reference to concepts associated with privacy, including a respect for human dignity, freedom of the individual to make decisions for themselves and be free from intrusion and intervention, respect for justice and due process, a commitment to equality and non-discrimination, and the right of citizens to access and participate in their governing processes and public services.

Following the ethical framework outlined in the previous section, in this section, we discuss specific challenges to privacy presented by twenty-first-century emerging technologies in order to illustrate the ways in which the contexts for privacy viola-

tions have become more complex. We organize these discussions around five ethical principles: *autonomy*, *justice*, *non-maleficence*, *beneficence*, and *explicability.*

While we continue to address concepts traditionally associated with privacy, such as anonymity, confidentiality, consent, right to correct, and minimization of scope, we argue here that privacy threats now encompass broader ethical concerns. Specifically, we suggest that ethical concerns in privacy must now shift:

- Beyond a focus on data protection of individuals to consider multifaceted and ubiquitous forms of surveillance as intrusions that violate respect for one's *dignity*
- From consent of individuals to a concern for human *agency* and *autonomy*
- From a focus on individual due process to a consideration of social fairness, non-discrimination, and *justice*
- From individual risk assessments to also consider safety, robustness, and the protection and inclusion of vulnerable populations as *non-maleficent* goals
- Beyond the individual or singular context of intrusion or data collection to consider collective responsibilities for environmental, social, and cultural well-being aligned with *beneficent* goals
- Beyond limits of scope and purpose to also consider data integrity, provenance, and accountability for *explicability* in the processes of algorithms, modeling, and data use

17.4.1 Autonomy as Dignity: From Data Protection to Multifaceted Forms of Intrusion

For the past 50 years, starting with the advent of computer systems used to store electronic records about individuals in financial, health, educational, and other sectors, the primary focus of privacy concerns has been the protection of data used in order to ensure that individual rights to privacy are not violated. Those concerns remain today, but they are complicated by the multiple forms of data that are now collected (e.g., numeric, text, voice, image, biometric) as well as the many technological means for doing so. We now live in a world filled with video cameras, facial recognition systems, RFID chips, electronic toll collectors, smartphones with location tracking, and voice-activated networks in our homes and automobiles. This modern context enables large-scale ubiquitous multimodal surveillance of users and citizens in public as well as in spaces traditionally considered to be private and free from intrusion: our cars, homes, and bedrooms. These new contexts suggest that ethical concerns in privacy must now shift beyond a focus on data protection of individuals to consider multifaceted and ubiquitous forms of surveillance as intrusions that violate respect for one's dignity, as an expression of individual autonomy. That includes concerns about privacy of one's *person*, *identity*, as well as one's *information*.

For example, facial recognition technologies (FRTs) used in public spaces present unique challenges for privacy. Using biometric data and processes to map facial features from image or video data, facial recognition systems attempt to identify individuals by matching their image against stored data. Biometric identifier data (fingerprints, iris, and face images) raise specific privacy concerns because they are uniquely identifiable, highly sensitive, and hard to secure. And if captured and misused, biometric data cannot be changed or uncoupled from an individual's identity [34]. When used by government or other institutional authorities to identify, track, and surveil citizens or institutional members, FRTs create fundamental imbalances in power and can be used as a means of social control, a form of digital authoritarianism [35].

For example, FRTs in China are an integral part of a social scoring system used to monitor and assess citizen behavior in public spaces and assign consequences when behaviors fall outside acceptable boundaries [36]. Similarly, the use of biometric identification systems in India's Aadhaar [37]—a centralized database that collects biometric information from 1.35 billion citizens, including fingerprints, iris scans, photographs, demographic information, and a unique 12-digit identifier—has raised significant concerns about the unprecedented access to and power over citizens given to government [38].

Because FRTs often operate continuously, invisibly, ubiquitously, and automatically, concerns about the risks of intrusion increase due to the large amounts of data collected, when data is collected without the knowledge or consent of the subject, and when human determination is removed from the equation. In addition, concerns about the accuracy, reliability, and security of FRTs—including false positives and negatives (e.g., for women and persons of color; [39])—have led some companies and countries to call for moratoriums on the use of FRTs in public spaces [40]. The specific risks of structural violence [41] resulting from the use of technologies to categorize individuals, monitor their movements, and mete punishments lead to clear potential loss of freedoms of movement, intrusion, and liberty.

17.4.2 Autonomy as Agency: From Consent to Access

A second, prominent privacy concern has centered around the expectation of *knowledge and consent* of an individual when her person or information is accessed. Individuals who provide permission to be searched or have their information collected are presumed to give *informed consent*—a fundamental assumption that individuals have the right to decide when, what, and how much information about themselves will be shared [42] or that they have *agency* in the decisions that are made on their behalf (see [43] on proxy consent; [44] on deferred consent). Consent and agency have formed the core elements of research ethics practice (see Common Rule) as well as terms of service used in many industries.

Yet while our early conceptions of consent were based on individual transactions, today's ubiquitous, invisible, and large-scale data collection practices mean consent

is not only difficult, it is largely no longer meaningful [45]. For example, when withholding consent equates to being denied access to services and goods provided through such platforms (e.g., without an Aadhaar ID, one cannot receive social support services), or when the terms of service agreements are inauthentic because they are too complex to be understandable or disguise exceptions that allow data sharing [46], consent as a means to respect and protect the rights of individuals to control their information becomes meaningless.

We argue that respecting autonomy in new privacy eras must shift away from consent and toward access, since self-governance is as much contingent on access (to *read*) as it is contingent on permission (to *be read*). This balance between read and write is essential in the context of information systems. We must ask not only *What is the role that individuals play in determining how data are used?* but also *What level of control do humans maintain in automated systems?* and *How are systems designed to gauge individual tolerance for trusted systems and to adjust if a potential intrusion (or trust-eroding event) is imminent?*

The ethical concern here focuses on tensions around autonomy between consent and agency. In addition to having the capability to act on the basis of one's own decisions and ensure that individuals are not placed at risk when sharing information [47], we must also have the agency to intervene when engaging with automated systems or decision-making algorithms that make determinations about us.

One example arises in self-driving vehicles. Because these systems are designed with granular levels of autonomy in decision-making and responses to environmental stimuli, they must also be designed to learn and adopt the values of the community in which they are installed. This is essential not only for trustworthiness but also to ensure the preservation of human determination. Thus, critically important is an iterative design process that continually assesses ethical consequences of design choices, follows *ethically aligned* standards [48], and ensures that individuals are able to determine the values and rules used in the process. Centering humans and their values in the loop is a key part of *human-centric computing* [49, 50], where technological devices, algorithms, and systems are designed with consideration of the human impact, and human values are centered in the design process (see also *value-sensitive design* [51] and *privacy by design* [52]).

17.4.3 Justice: From Material Risk to Fairness and Due Process

In light of growing evidence and concerns about unfairness in technologies and algorithms, there have been many recent calls to reorient and broaden ethics discussion about emerging technologies like AI, as one that is defined by *justice*, including social, racial, economic, and environmental justice [53, 54]. Others have taken up these concerns as *information justice* (e.g., [55, 56]) or *algorithmic justice* [57] (see https://www.ajl.org/).

These discussions focus on the technical mechanisms needed to address questions of fairness, bias, and discrimination in algorithmic systems, as well the consequences suffered by individuals and groups from inaccurate, unfair, or unjust systems. With the deployment of predictive algorithms and machine-learning models as decision-support systems across many sectors—e.g., financial, health, and judicial—these consequences are of great concern [58].

For example, the work of Buolamwini and Gebru [39] revealed that a widely used facial recognition system was largely inaccurate in identifying darker-skinned females, with error rates close to 35%, compared to 1% for lighter-skinned males – suggesting that automated facial analysis algorithms and datasets can produce both gender and racial biases. Similarly, a widely used predictive algorithm used by judicial courts in the United States to predict recidivism rates for sentencing decisions was found to be more likely to incorrectly label Black defendants as higher risks compared to White defendants [59]. These cases illustrate the larger societal risks that arise from algorithmic decisions that lead to systematic bias against individuals within groups with protected social identities like race, gender, and sexuality [60, 61].

Even for non-marginalized populations, algorithmic bias can lead to decisions that limit opportunities, intentionally or not. When Amazon attempted to address gender gaps in its hiring, they implemented an applicant screening algorithm to predict applicants likely to match the qualities of past successful candidates [62]. But when the outcome widened gender gaps, they realized the dataset used to train the model included primarily successful *male employees*, thus making it less likely that *female applicants* would match the ideal [63]. In this case, the problem was not inaccuracies in the data or model but rather what was *missing*: there was insufficient data about females to model a fair representation of their goals [64].

Algorithmic bias has due process implications as well. For example, automated performance evaluation systems for public school teachers in California, New York, and Texas led to termination decisions, without informing the employees such tools were being used or providing meaningful opportunities for scrutiny and accountability. Such secret black box systems, especially in public agencies, generate a number of ethical concerns [65, 66].

On a societal level, the use of social credit scoring systems (SCS) also carries the potential for large-scale systematic violations of privacy and human rights. In China, a government-mandated SCS was implemented to strengthen social governance and harmony [67]. Every citizen was assigned a "trustworthiness" score, calculated from an algorithmic assessment of data from medical, insurance, bank, and school records; credit card and online transactions; satellite sensor data; mobile phone GPS data; and behavioral data from public cameras. Authorities use these data and the social credit score to evaluate and hold citizens accountable by imposing sanctions that range from restrictions on travel, bans on employment in civil service and public institutions, disqualification of children from private schools, and public disclosure of ratings on national websites [68]. Thus, the stakes of large-scale state surveillance include significant loss of freedoms of movement, employment, education, and reputation [41].

17.4.4 Non-maleficence and Beneficence: From Individual Risk to Collective Societal Good

17.4.4.1 Non-maleficence

Privacy ethics have long included attention to assessing the risk for individuals and adequately consider the safety, robustness, and protection of vulnerable populations. Indeed, much of the legal discourse about privacy protection and rights centers on the harmful consequences suffered when privacy is violated. However, harm remains narrowly defined and allows violations to go unpunished. In this section, we argue that broadening the ethical focus to one of *non-maleficence* — a call to ensure that our research conduct and technological designs also consider potential harms to society at large—provides an opportunity to broaden concerns beyond individual risk assessments to consider and assess long-term social, intellectual, and political consequences.

At the intersections of humans and technologies, there are significant privacy concerns, in particular for the young (Chap. 14 this volume), the vulnerable (Chap. 15, this volume) and the marginalized, that are exacerbated with contemporary technologies. Of specific concern are tools of authoritarian regimes that have clear and dangerous consequences when individuals can more easily be identified and targeted [35]. For example, it has recently come to light that facial recognition and other surveillance technologies are being used to identify, persecute, and imprison members of the Uyghur population in China [69]. Members of this community are considered enemies of the Communist Party and subjected to incarceration and, by some reports, torture, sterilization, and starvation. The determination of whether Uyghurs are imprisoned is built upon a massive system of government surveillance both in public spaces using a network of CCTV cameras equipped with facial recognition software as well as private spaces using spyware installed on smartphones, allowing the government to trace location, communication, and media use [70].

Another example of malicious, harmful technology is illustrated in the case of deepfake technologies. Deepfake technology uses machine learning algorithms to combine images and voices from one person into recordings of another to create a realistic impersonation that is difficult to detect as inauthentic. Doctoring images is not new, nor are harmful lies. But as Floridi [71] notes, deepfake technologies can also "undermine our confidence in the original, genuine, authentic nature of what we see and hear" (p. 320).

The sophisticated digital impersonation made possible with modern deepfake technologies is realistic and convincing in a way that carries the potential for significant harms. Typically created without the knowledge or consent of the individual and often in negative or undesirable situations, they present significant ethical violations and a wide array of harms. These harms include *economic* harms from extortions under threat to release the videos; *physical* and *emotional* harms from simulated violence and dignitary or *reputational* harms that include

relationship loss, job loss, and stigmatization in one's community; and even *societal* harms when important political figures are depicted in damaging contexts, election results are manipulated, or trust is eroded in critical institutions [72]. As more of our identities shift into digital spaces, this array of harms is informationalized or spread beyond the bodily self to the networks of information that extend us digitally [15]. Thus, the potentials for harm are significantly amplified in a networked information environment context that facilitates wide distribution, viral spread, and infinite persistence of access.

17.4.4.2 Beneficence

If non-maleficence asks moral agents merely to avoid harms, the principle of *beneficence* shifts our focus to a positive account of doing good. Beneficence implies a balancing of tensions between individual and collective concerns to consider how we can design and conduct our research with a specific goal to benefit the well-being of society. This requires moving beyond the individual in a singular context of intrusion or data collection to consider collective responsibilities for environmental, social, and cultural well-being aligned with beneficent goals.

In the research context, this means asking not only *How do I avoid risks*? but also *How can I modify how I conduct my work so that it generates social good and contributes to well-being*? In the industry context, there have been growing movements to promote the specific design and deployment of technologies to serve broader social good—ICT4All and, for example AI4Good—particularly focusing on technologies to contribute to the social and economic development of underserved populations and countries [71]. Other calls have come from disciplines like human-computer interaction to discuss emerging policy needs for culturally sensitive HCI, accessible interactions, and the environmental impact of HCI [73].

The principles of non-maleficence and beneficence intersect as privacy practices and policies continue to negotiate value tensions between avoiding harms and managing risk and active engagement in developing or protecting privacy concerns. One example is the technologies and applications developed to minimize the risk and spread of infection during the COVID-19 pandemic. In order to manage the highly infectious disease, public health officials around the world raced to create technological and data analysis capabilities, including contact tracing, symptom tracking, surveillance, and enforcement of quarantine orders—typically enabled through mobile phones [74]. These health surveillance systems provide important capability to mitigate and manage the risks to global public health during the pandemic but also raise concerns about potential individual and societal-level privacy violations, both short term and long term. They seek to balance potential privacy harms against the good of public health.

Short-term concerns focus on the sharing of highly sensitive health, location, and behavioral data, complicated with disclosures of infectious health status. Long-term concerns center around the ambiguous end point for data collection and concerns that once allowed in order to mitigate a temporary emergency, surveillance

will become permanent. Unfortunately, these concerns are warranted based on the history of previous surveillance activities enacted during crises: In the United States, there have been over 30 national emergencies declared providing emergency powers, including the domestic and international surveillance activities put in place after the September 11 terrorist attacks [75]. Balancing the clear long-term societal benefit of technologies to manage critical infection spread and reduce deaths and health-care costs, with short-term risks of disclosing sensitive personal information and long-term risks of continuous health surveillance, illustrates the ethical tensions of crisis contexts.

17.4.5 Explicability: From Data Transparency to Process Intelligibility

Ethical values are always tightly coupled to epistemic values, or values about what and how we know. Privacy ethics have long focused on the important epistemic principles of *transparency* (i.e., providing notice to individuals regarding the collection, use, and dissemination of personally identifiable information), as well as *accountability* (i.e., holding accountable compliance with privacy protection requirements) [76]. In the modern era, where the workings "inside the box" of complex systems are often invisible or unintelligible to most, these principles must be broadened to include requirements for *intelligibility (how does it work?)*, along with clear provenance of the data and people involved (*who is responsible for the way it works?*) [77].

Collectively this principle has been termed *explicability*, or the ability to obtain a clear and direct explanation of a decision-making process [71], cf. [78]. Explicability is especially salient in the case of algorithms and machine learning procedures and ensures individuals the right to know and understand what led to decisions that have significant consequence in their liberty, employment, and economic well-being: freedoms that are fundamental human rights protected by law.

Furthermore, as Floridi and Cowls [77] explain, explicability actually complements (or *enables*) the other principles: In order for designers and researchers to not constrain human *autonomy* and "keep the human in the loop," we must know how the technologies might act or make decisions (instead of us) and when human intervention or oversight is required; to assure *justice*, we need to be able to identify who will be held accountable and explain why there was a negative consequence, when there are unjust outcomes; and to adhere to values of *beneficence* and *non-maleficence*, we must understand how such technologies will benefit or harm our society and environment (p. 700).

Pasquale's *Black Box Society* [65] makes clear that algorithmic decision-making produces morally significant decisions with real-life consequences in employment, housing, credit, commerce, and criminal sentencing often without offering an explanation for how such decisions were reached. Civil society advocates have

warned that "many of these techniques are entirely opaque, leaving individuals unaware whether the decisions were accurate, fair, or even about them" [79].

For example, algorithms are used in the criminal justice system to predict the probability of recidivism for individuals in parole and sentencing decisions. One such tool, the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), has been used in more than 1 million cases since 1998, yet research indicates the accuracy of predictions made by the algorithm is no more accurate than those made by people without criminal justice expertise [80]. Furthermore, although individuals are more likely to trust the accuracy of computational tools, research indicates the COMPAS tool led to racially-biased outcomes: it overestimated the rate at which Black defendants would reoffend and underestimated the rate at which White defendants would [59, 81]. Furthermore, when defendants challenged the decisions, they were unable to receive an explanation about the information used in the decision because the COMPAS creators claimed the algorithm was proprietary information [82]. In doing so, they violated the defendant's right to due process.

The factual context of a particular privacy problem is a key element of specifying ethical principles. The epistemic context is always tightly coupled to the ethical. In privacy eras of varying complexities, the explicability of data has an impact not only on the reception of ethics but also on the transmission: especially when artificial agents are included in those contexts. Like other ethical principles, the epistemic principle of explicability takes on an increasingly complex role. Whether in the context of predictive algorithms, surveillance by autonomous systems, or any other information context, epistemic values no longer merely focus on replicability or accuracy but instead on validity, transparency, and comprehensibility.

Emerging ethical challenges to core ethical principles shift the way principles are specified and balanced, adding complexity to their scope and focus. These challenges have direct implications for research policy and practice.

17.5 Guidelines for Research and Practice

In this next section, we connect the theoretical and applied to the practical, considering how an ethics literate perspective on privacy can inform the future of related policy and regulatory discussions (see [83]). While having the tools to engage with ethical principles has utility in the face of emerging technologies and unformed social norms, researchers and practitioners are still well served with additional resources for guidance in ethical decision-making.

Having worked through the reasons and justifications offered by ethical principles and frameworks, one might still ask how that work connects, practically, to our world bound by law and policy. Law and regulation provide actionable guidance and rules for professional conduct and technological development, codifying the reasoning outcomes of ethics. For example, the Privacy Act (1974), [27, 84] provide federal law to govern the collection, use, and dissemination of personally

identifiable information in federal, health insurance, and telecommunication records in the United States; the Illinois Biometric Privacy Act (2008) extends protections to residents of the state of Illinois for biometric data; and the GDPR [85] provides regulatory protection of personal data for citizens of the European Union (see Chap. 18 for a review).

In research practice in the United States, ethical conduct for federally funded research involving human participants is guided by the Belmont Report [86], which applies the principles of beneficence, justice, and respect for persons to research practice. To assure compliance with these ethical guidelines, the Common Rule [87] codifies federal regulations for the protection of human subjects, with additional protections for vulnerable populations. Industry researchers are also typically required to abide by institutional policies or guidelines established for ethical practice (e.g., [88–90]).

Laws and regulations provide specific rules for ethical conduct and practice but can be dated in their relevance to today's technological contexts. Nearly 50 years have passed since the earliest privacy laws, and 30 years since the publication of the Common Rule, so there are inherently *gaps* in the relevance of legal and ethical guidelines established when computational technologies were in their infancy. Furthermore, the development of new law or international treaties takes time, resources, and significant negotiation, which means that "hard law" often lags behind the pace of development for innovative technologies (the "pacing problem"; [91]). For example, governments around the world are working to develop policy for the governance of AI technologies, as industries race to become global leaders in this field. Still others, such as the United States, have not yet passed comprehensive privacy legislation to address the unique challenges of modern contexts and technological capabilities.

These *gaps* in codified law and regulatory guidelines create challenges for researchers and designers when the technologies being tested and implemented are not specifically addressed. As we move into new eras, new contexts and technologies create new uncertainties in ethical decisions. However, "soft law" can fill the gaps until such hard codes are in place, or even where hard laws and regulations are in conflict with one another [91]. Wallach and Marchant [92] note that soft law measures—including technical standards, codes of conduct, curricular programs, and statements of principles—can also be promulgated by many stakeholders including "governments, industry actors, nongovernmental organizations, professional societies, standard-setting organizations, think tanks, public–private partnerships, or any combination of the above" (p. 506). Thus, soft law serves as an important complement to hard-coded law and regulation—particularly when norms and technologies are still developing.

17.5.1 Technical Standards

In some cases, there are government or industry *standards* available to provide specific guidance. For example, the National Institute of Standards and Technology

(NIST) in the United States provides industry standards for technologies, including a *privacy framework* guidebook for enterprise risk management [14]. In addition, the Institute of Electrical and Electronics Engineers (IEEE) professional society is a leading source for standards for emerging technologies with over 1300 standards [48] such as one for *data privacy* (P7002), recommended practice for *inclusion, dignity, and privacy in online gaming* (P2876), and one under development for *biometric privacy* (P2410). They have also published a resource guide for *ethically aligned design* for human well-being in autonomous and intelligent systems (IEEE EAD 2017).

17.5.2 Statements of Principles

Another set of resources are available in the form of *statements of principles* developed by scientific societies (e.g., ACM, AAAS, IEEE), civil society organizations (e.g., Electronic Privacy Information Center), think tanks (e.g., AI Now Institute), or government agencies. These principles are amalgams of value concerns identified by members of a specific community. One well-known set of principles for privacy researchers are the *Fair Information Practices* first published in 1973 through the US Department of Health, Education, and Welfare [76]. These included the now familiar concepts of *notice*, *consent*, *access*, *security*, and *redress* and laid important groundwork for subsequent legislation. The ACM professional society for computer scientists also releases regular policy statements on emerging technologies (see https://www.acm.org/public-policy), such as its *Statement of Privacy Principles* [93, 94], which outlines foundational principles of *fairness*, *transparency*, *collection limits*, *control*, *security*, *data integrity and retention*, and *risk management.*

Most recently, a number of principles have been released to address ethics for AI technologies (see [20]). The most significant is the Principles on AI released by the international Organisation for Economic Co-operation and Development [95]. These guidelines identified five values-based principles for trustworthy AI that closely align with *beneficence*, *justice*, *transparency*, *security*, and *accountability*. The OECD principles were subsequently endorsed by the G20 leaders in 2020, providing an important international agreement. In addition, global technology industries, such as Google, Microsoft, and IBM, have also contributed AI Principles to communicate to their clients and employees that their practices and technologies will be designed and implemented in ways that are trustworthy and adhere to consensus principles [88–90].

17.5.3 Codes of Conduct

Codes of ethics and professional conduct can also provide helpful guidance regarding practices specific to your profession. Some spell out clear consequences

for conduct outside the bounds of acceptable behavior and practice (e.g., loss of funding, loss of rights to conduct research, loss of licensure, or loss of employment). For example, the ACM Code of Ethics [93] includes seven ethical imperatives and 18 professional responsibilities for those practicing in computer professions, including *respect for privacy and confidentiality*, *avoid harm*, *be fair and not discriminate*, and *contribute to human well-being* that again resonate with the principles outlined in this chapter [96].

17.5.4 Curricular Programs

Finally, curricular innovations are another approach under the umbrella of soft law. Public attention to questions of privacy and information ethics more generally has yielded calls for parallel attention to ethics education curricula at the collegiate level, in disciplines of computer science, engineering, and data science. To date, disciplines have been slow to integrate ethics modules or courses into their undergraduate and graduate curriculums (cf. [97, 98]). However, some early examples include the PRIME Ethics program developed for graduate students in science and engineering [12], which combines the reflexive principlism framework with discipline-specific case studies to strengthen ethical reasoning skills [99, 100]. In computer science, colleagues are beginning to develop ethics education activities for CS courses [101], and other universities, such as the Markkula Center for Applied Ethics, have developed ethics education modules for data ethics, software engineering, and technology practice (see https://www.scu.edu/ethics/ethics-resources/ethics-curricula/).

17.6 Conclusion

In this work, we asked: *What are the ethics of conducting privacy research and technology design, what new challenges do we face with next-generation technologies like AI, and how do the core questions we have relied upon for decades change in these new contexts?* To answer those questions, we argued that the contexts of sociotechnical privacy have evolved significantly in 50 years, with correlate shifts in the norms, values, and ethical concerns, and this has yielded significant eras of privacy (from 1.0 to 5.0), each with a broadening field of ethical concerns. We discussed these emerging ethical issues and introduced a *principlist framework* for privacy researchers to guide ethical decision-making. To summarize, we discussed that:

- Contexts of privacy have expanded from individual (1.0) to internet (2.0), to interdependence (3.0), to intelligences (4.0), to artificiality (5.0).

- Effective ethical decision-making (EDM) approaches are pluralistic, involving interface among ethical and epistemic principles as privacy paradigms evolve.
- Contemporary relationships between moral patients (receivers) and moral agents (transmitters) are shaped by digital information.
- Principles are reflexively applied in the ethical-decision making process.

We then discussed specific emerging privacy challenges and used the principlist framework to reframe privacy concerns amidst these emerging contexts and ethical questions, organizing the discussions around five ethical principles. To summarize, we discussed that:

- *Autonomy* shifts from data protection to multifaceted forms of intrusion and access.
- *Justice* shifts from material risk to fairness and due process.
- *Non-maleficence* and *beneficence* shift from individual harms to collective societal good.
- *Explicability* shifts from data transparency to process intelligibility.

Finally, we noted that while having the conceptual and reasoning tools to engage with ethical principles has utility in the face of emerging technologies and unformed social norms, researchers and practitioners are also well served with additional resources for guidance in ethical decision-making. We then briefly discussed soft law resources that can provide practical guidance in ethical decision-making, including technical standards, codes of ethical conduct, curricular programming, and statements of principles.

As researchers, we have an ethical obligation to ensure our research practice does not create undue intrusion on the people involved and that our results advance scientific knowledge to inform better practice. As designers, we have an ethical obligation to ensure the algorithms, applications, devices, and platforms we design yield intelligent agents that act and behave morally and contribute to the larger social good.

The notion of privacy is not dead but instead reborn in new form in the digital era: a fundamental human right deserving of protection and possibly under greater threat than any time of modern technological development. Striving for control of our own information, the right to manage it, strategies for understanding it and applying it fairly, and policies and practices to balance its harms and benefits will continue to be key foci of the ethics of privacy. But the mechanisms for intrusion on one's space, person, and identity are vastly more complex today than they were in the eras of Warren and Brandeis [102] and Westin [42], and the ethical concerns that come into play when we consider privacy ethics have now also broadened. Guidance for ethical decision-making, grounded in ethical principles, is a necessary tool in this challenging future.

References

1. Spector-Bagdady, K., and P.A. Lombardo. 2013. "Something of an adventure": Postwar NIH research ethos and the Guatemala STD experiments. *The Journal of Law, Medicine & Ethics* 41 (3): 697–710. https://doi.org/10.1111/jlme.12080.
2. Hudson, K.L., and F.S. Collins. 2013. Family matters. *Nature* 500 (7461): 141–142. https://doi.org/10.1038/500141a.
3. Skloot, R. 2018. *Immortal Life of Henrietta Lacks*. New York, NY: Crown.
4. Beauchamp, T.L., and J.F. Childress. 2019. *Principles of Biomedical Ethics*. 8th ed. Cambridge, UK: Oxford University Press.
5. Richardson, H.S. 2000. Specifying, balancing, and interpreting bioethical principles. *The Journal of Medicine and Philosophy* 25 (3): 285–307. https://doi.org/10.1076/0360-5310(200006)25:3;1-h;ft285.
6. Beever, J., and A.O. Brightman. 2015. Reflexive principlism as an effective approach for developing ethical reasoning in engineering. *Science and Engineering Ethics* 22 (1): 275–291. https://doi.org/10.1007/s11948-015-9633-5.
7. Steneck NH. 2019. *Introduction to the Responsible Conduct of Research*. Office of Research Integrity, Department of HHS. https://ori.hhs.gov/ori-introduction-responsible-conduct-research. Accessed 19 Feb 2021.
8. Nissenbaum, H.F. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.
9. 398 U.S. 347. 1967. *Katz v. United States, 389*. Retrieved from https://supreme.justia.com/cases/federal/us/389/347/.
10. 5 U.S.C. Sec 552a. 1974. *The Privacy Act of 1974*. Retrieved from https://www.justice.gov/opcl/privacy-act-1974
11. Floridi, L. 2015. *The Ethics of Information*. Oxford, UK: Oxford University Press.
12. Brightman, A., J. Beever, J. Hess, A. Iliadis, L. Kisselburgh, M. Krane, M. Loui, and C. Zoltowski. 2016. PRIME ethics: Purdue's reflective & interactive modules for engineering ethics. In *Infusing Ethics into the Development of Engineers: Exemplary Education Activities and Programs*, ed. National Academy of Engineering, 39–40. Washington, DC: National Academies Press.
13. Laney D. 2012. *Deja VVVu: Gartner's Original "Volume-Velocity-Variety" definition of big data*. https://community.aiim.org/blogs/doug-laney/2012/08/25/deja-vvvu-gartners-original-volume-velocity-variety-definition-of-big-data. Accessed 18 Feb 2021.
14. ———. 2018. *Privacy Framework*. National Institute for Standards and Technology. https://www.nist.gov/privacy-framework. Accessed 18 Feb 2021.
15. Kisselburgh, L. 2011. Privacy in networks. In *Encyclopedia of Social Networks*, ed. G. Barnett and J.G. Golson. Sage.
16. Beever, J. 2021. *Philosophy, Film, and the Dark Side of Interdependence*. Lanham, MD: Lexington Books.
17. Caine, K., L. Kisselburgh, and L. Lareau. 2011. Audience visualization influences online social network disclosure decisions. In *CHI EA 2011: Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems*, 1663–1668. New York: ACM.
18. Kisselburgh, L. 2012. Privacy and social media ecologie. In *CSCW'12 Conference on Computer-Supported Cooperative Work*. New York, NY: ACM.
19. Lipford HR, Wisniewski P, Lampe C, Kisselburgh L, Caine K (2012) Reconciling privacy with social media. In *Proceedings of the 2012 Annual Conference on Computer-supported Cooperative Work Companion*, pp. 19–20.
20. Jobin, A., M. Ienca, and E. Vayena. 2019. The global landscape of AI ethics guidelines. *Nature Machine Intelligence* 1 (9): 389–399. https://doi.org/10.1038/s42256-019-0088-2.
21. Cottone, R.R., and R.E. Claus. 2000. Ethical decision-making models: A review of the literature. *Journal of Counseling and Development* 78 (3): 275–283. https://doi.org/10.1002/j.1556-6676.2000.tb01908.x.

22. Tuana, N. 2014. An ethical leadership development framework. In *The Handbook of Ethical Educational Leadership*, ed. C.M. Branson and S.J. Gross, 153–175. Hoboken, NJ: Taylor and Francis.
23. ———. 2007. Conceptualizing moral literacy. *Journal of Educational Administration* 45 (4): 364–378. https://doi.org/10.1108/09578230710762409.
24. Kuebler S, and Beever J. 2019 Who should self-driving cars be programmed to protect? UCF forum 339.
25. Smith A. 2020. Should we recognize privacy as a human right? In *National Magazine*. http://nationalmagazine.ca/en-ca/articles/law/in-depth/2020/should-we-recognize-privacy-as-a-human-right. Accessed 16 Feb 2021.
26. Beauchamp, T.L. 1995. Principlism and its alleged competitors. *Kennedy Institute of Ethics Journal* 5 (3): 181–198. https://doi.org/10.1353/ken.0.0111.
27. The Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996).
28. Carter, S.M., W. Rogers, K.T. Win, H. Frazer, B. Richards, and N. Houssami. 2020. The ethical, legal and social implications of using artificial intelligence systems in breast cancer care. *The Breast* 49: 25–32. https://doi.org/10.1016/j.breast.2019.10.001.
29. Gao, Y., K.J. Geras, A.A. Lewin, and L. Moy. 2019. New frontiers: An update on computer-aided diagnosis for breast imaging in the age of artificial intelligence. *American Journal of Roentgenology* 212 (2): 300–307. https://doi.org/10.2214/AJR.18.20392.
30. Brožek, B., and B. Janik. 2019. Can artificial intelligences be moral agents? *New Ideas in Psychology* 54: 101–106. https://doi.org/10.1016/j.newideapsych.2018.12.002.
31. Bari, L., and D.P. O'Neill. 2019. Rethinking patient data privacy in the era of digital health. *Health Affairs*.
32. Nietzsche F. 2016/1885. *Thus spake Zarathustra: A book for all and None*. Thomas common (trans. https://www.gutenberg.org/files/1998/1998-h/1998-h.htm. Retrieved 1 May 2021.
33. United Nations. 1948. *The Universal Declaration of Human Rights*. https://www.un.org/en/universal-declaration-human-rights/. Accessed 19 Feb 2021.
34. Kak A. 2020. *Regulating Biometrics: Global Approaches and Urgent Questions*. AI Now Institute. https://ainowinstitute.org/regulatingbiometrics.pdf. Accessed 18 Feb 2021.
35. Polyakova A, and Meserole C. 2019. *Exporting Digital Authoritarianism: The Russian and Chinese Models*. Brookings Institute. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf
36. Kostka, G., L. Steinacker, and M. Meckel. 2020. Between privacy and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the UK and the US. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3518857.
37. Banerjee, S., and S. Sharma. 2019. Privacy concerns with Aadhaar. *Communications of the ACM* 62 (11): 80–80. https://doi.org/10.1145/3353770.
38. Ranganathan, N. 2020. The economy (and regulatory practice) that biometrics inspires: A study of the Aadhaar project. In *Regulating Biometrics: Global Approaches and Urgent Questions*, ed. A. Kak, 52–61. New York: AI Now Institute.
39. Buolamwini, J., and T. Gebru. 2018. Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research* 81: 1–15.
40. Pasquale, F. 2018. When machine learning is facially invalid: Observations on the use of machine learning and facial inferences to classify people using inexplicable data. *Communications of the ACM* 61 (9): 25–27.
41. ———. 2020. *New Laws of Robotics Defending Human Expertise in the Age of AI*. Cambridge, MA: Harvard University Press.
42. Westin, A.F. 1970. *Privacy and Freedom*. New York: Atheneum.
43. Saks, E., L. Dunn, J. Wimer, M. Gonzales, and S. Kim. 2013. Proxy consent to research: The legal landscape. *Yale Journal of Health Policy, Law, and Ethics* 8 (1): 37–92.
44. Levine, R.J. 1995. Research in emergency situations. The role of deferred consent. *JAMA-J Am Med Assoc* 273 (16): 1300–1302. https://doi.org/10.1001/jama.273.16.1300.

45. Nissenbaum, H.F. 2018. Stop thinking about consent: It isn't possible and it isn't right. *Harvard Bus Review*, 19–22.
46. Fiesler, C., N. Beard, and B.C. Keegan. 2020. No robots, spiders, or scrapers: Legal and ethical regulation of data collection methods in social media terms of service. *Proceedings of the International AAAI Conference on Web and Social Media* 14: 187–196.
47. Friedman, B., and H. Nissenbaum. 1996. User autonomy: Who should control what and when? In *CHI '96: Conference Companion on Human Factors in Computing Systems*. New York: ACM.
48. IEEE. 2018. Ethically aligned design: A vision for prioritizing human well-being with autonomous and intelligent systems. https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead_v2.pdf. Accessed 18 Feb 2021.
49. Dow K, and Hancock M. 2018. *Injecting Ethical Considerations in Innovation via Standards – Keeping Humans in the AI Loop*. IEEE Insight. https://insight.ieeeusa.org/articles/standards-address-ai-ethical-considerations/.
50. Shneiderman, B. 2020. Bridging the gap between ethics and practice. *ACM Transactions on Interactive Intelligent Systems* 10 (4): 1–31. https://doi.org/10.1145/3419764.
51. Friedman, B., and P.H. Kahn. 2007. Human values, ethics, and design. In *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies and Emerging Application*, ed. A. Sears and J.A. Jacko, 2nd ed., 1177–1201. Boca Raton: CRC Press.
52. Cavoukian A. 2009 Privacy by design: The seven foundational principles. https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/. Accessed 18 Feb 2021.
53. Ada Lovelace Institute. 2020. Examining the black box: Tools for assessing algorithmic systems. https://www.adalovelaceinstitute.org/report/examining-the-black-box-tools-for-assessing-algorithmic-systems/. Accessed 18 Feb 2021.
54. Hao K. 2021. *Deepfake Porn Is Ruining Women's Lives. Now the Law May Finally Ban It*. MIT Technology Review. https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming-ban/. Accessed 15 Feb 2021.
55. Butcher, M.P. 2009. At the foundations of information justice. *Ethics and Information Technology* 11 (1): 57–69. https://doi.org/10.1007/s10676-009-9181-2.
56. O'Neil, C. 2018. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. London: Penguin Books.
57. Re, R.M., and A. Solow-Niederman. 2019. Developing artificially intelligent justice. *Stanford Technology Law Review* 22: 242.
58. Binns, R. 2018. Fairness in machine learning: Lessons from political philosophy. *Proceedings of Machine Learning Research* 81: 149–159.
59. Angwin J, Larson J, Mattu S, Kirchner L. 2016. *Machine Bias*. ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Accessed 18 Feb 2021.
60. Noble, S.U. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press.
61. Ferguson, A.G. 2019. *Rise of Big data policing: Surveillance, race, and the future of law enforcement*. New York, NY: New York University Press.
62. Hamilton, R.H., and W.A. Sodeman. 2019. The questions we ask: Opportunities and challenges for using big data analytics to strategically manage human capital resources. *Business Horizons* 63 (1): 85–95. https://doi.org/10.1016/j.bushor.2019.10.001.
63. Reuters. 2018. Amazon ditched AI recruiting tool that favored men for technical jobs. In *The Guardian*. https://www.theguardian.com/technology/2018/oct/10/amazon-hiring-ai-gender-bias-recruiting-engine. Accessed 18 Feb 2021.
64. Williams, B.A., C.F. Brooks, and Y. Shmargad. 2018. How algorithms discriminate based on data they lack: Challenges, solutions, and policy implications. *Journal of Information Policy* 8: 78–115. https://doi.org/10.5325/jinfopoli.8.2018.0078.
65. Pasquale, F. 2016. *Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge, MA: Harvard University Press.

66. Reisman D, Schultz J, Crawford K, and Whittaker M. 2018. Algorithmic impact assessments: A practical framework for public agency accountability. In *AI Now Institute*. https://ainowinstitute.org/aiareport2018.pdf. Accessed 16 Feb 2021.
67. Botsman R. 2017. *Big Data Meets Big Brother as China Moves to Rate Its Citizens*. WIRED. https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion. Accessed 18 Feb 2021.
68. Chen, Y., and A.S.Y. Cheung. 2017. The transparent self under big data profiling: Privacy and Chinese legislation on the social credit system. *SSRN Electronic Journal* 12 (2): 25–27. https://doi.org/10.2139/ssrn.2992537.
69. Mozur P. 2019. *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*. The New York Times. https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html. Accessed 18 Feb 2021.
70. Roberts, S.R. 2020. *The War on the Uyghurs China's Campaign Against Xinjiang's Muslims*. Manchester, UK: Manchester University Press.
71. Floridi, L., J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, C. Luetge, R. Madelin, U. Pagallo, F. Rossi, B. Schafer, P. Valcke, and E. Vayena. 2018. AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines* 28 (4): 689–707. https://doi.org/10.1007/s11023-018-9482-5.
72. Citron, D.K., and R. Chesney. 2019. Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review* 107: 1753. https://doi.org/10.2139/ssrn.3213954.
73. Kisselburgh, L., M. Beaudouin-Lafon, L. Cranor, J. Lazar, and V. Hanson. 2020. HCI ethics, privacy, accessibility, and the environment: A town hall forum on global policy issues. In *CHI2020: Proceedings of the 38th Annual CHI Conference on Human Factors in Computing Systems*. Honolulu, HI: ACM.
74. Li, T. 2020. Privacy in pandemic: Law, technology, and public health in the COVID-19 crisis. *SSRN Electronic Journal* 52 (3). https://doi.org/10.2139/ssrn.3690004.
75. Boudreaux, B., M.A. Denardo, S.W. Denton, R. Sanchez, K. Feistel, and H. Dayalani. 2020. Data privacy during pandemics: A scorecard approach for evaluating the privacy implications of COVID-19 mobile phone surveillance programs. RAND Corporation.
76. U.S. Department of Health, Education and Welfare. 1973. *The Code of Fair Information Practices.* Secretary's advisory committee on automated personal data systems, records, computers, and the rights of citizens viii.
77. Floridi, L., and J. Cowls. 2019. A unified framework of five principles for AI in society. *Harvard Data Science Review* 1 (1). https://doi.org/10.1162/99608f92.8cd550d1.
78. Robbins, S. 2019. A misdirected principle with a catch: Explicability for AI. *Minds and Machines* 29 (4): 495–514. https://doi.org/10.1007/s11023-019-09509-3.
79. The Public Voice. 2018. *Universal Guidelines for AI*. https://thepublicvoice.org/ai-universal-guidelines/. Accessed 19 Feb 2021.
80. Dressel, J., and H. Farid. 2018. The accuracy, fairness, and limits of predicting recidivism. *Science Advances* 4 (1): aao5580. https://doi.org/10.1126/sciadv.aao5580.
81. Barocas, S., and A.D. Selbst. 2016. Big Data's disparate impact. *California Law Review* 104 (3): 671–732. https://doi.org/10.2139/ssrn.2477899.
82. Loomis v. Wisconsin, 881 N.W.2d 749 (Wis. 2016), cert. denied, 137 S.Ct. 2290 (2017).
83. Diamantopoulou and King, this volume.
84. The Family Educational Rights and Privacy Act (FERPA) of 1974 (20 U.S.C. § 1232g; 34 CFR Part 99).
85. European Parliament and Council of European Union. 2016. *Regulation (EU) 2016/679*. ("General Data Protection Regulation"). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
86. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. 1979. *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research*.

87. 45 CFR Part 46. 1991. Federal policy for the protection of human subjects ("the Common Rule").
88. IBM. 2018. *IBM'S Principles for Data Trust and Transparency*. IBM. https://www.ibm.com/blogs/policy/trust-principles/. Accessed 15 Feb 2021.
89. Microsoft. 2018. Responsible AI principles from Microsoft. https://www.microsoft.com/en-us/ai/our-approach-to-ai. Accessed 18 Feb 2021.
90. Pichai S. 2018. AI at Google: Our principles. https://www.blog.google/technology/ai/ai-principles/. Accessed 18 Feb 2021.
91. Marchant, G.E. 2011. The growing gap between emerging technologies and the law. In *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem*, ed. G.E. Marchant, B.R. Allenby, and J.R. Herkert, 19–33. Cham: Springer.
92. Wallach, W., and G. Marchant. 2019. Toward the agile and comprehensive international governance of AI and robotics. *Proceedings of the IEEE* 107 (3): 505–508. https://doi.org/10.1109/jproc.2019.2899422.
93. Association for Computing Machinery. 2018. ACM code of ethics and professional conduct. https://www.acm.org/code-of-ethics. Accessed 18 Feb 2021.
94. USACM. 2018. Statement on the importance of preserving personal privacy. In *Association of Computing Machinery*. https://www.acm.org/binaries/content/assets/public-policy/2018_usacm_statement_preservingpersonalprivacy.pdf. Accessed 15 Feb 2021.
95. Organisation for Economic Co-operation and Development. 2019. Principles on artificial intelligence. https://www.oecd.org/going-digital/ai/principles/. Accessed 18 Feb 2021.
96. Gotterbarn, D., A. Bruckman, C. Flick, K. Miller, and M.J. Wolf. 2018. ACM code of ethics: A guide for positive action. *Communications of the ACM* 61 (1): 121–128. https://doi.org/10.1145/3173016.
97. Beever J, Kuebler SM, Collins J (2021) Where ethics is taught: An institutional epidemiology. *International Journal of Ethics Education* 6 (2): 215–238.
98. Karoff P. 2019. *Harvard Works to Embed Ethics in Computer Science Curriculum*. Harvard Gazette. https://news.harvard.edu/gazette/story/2019/01/harvard-works-to-embed-ethics-in-computer-science-curriculum/. Accessed 15 Feb 2021.
99. Hess, J.L., J. Beever, C.B. Zoltowski, L. Kisselburgh, and A.O. Brightman. 2019. Enhancing engineering students' ethical reasoning: Situating reflexive principlism within the SIRA framework. *Journal of Engineering Education* 108 (1): 82–102. https://doi.org/10.1002/jee.20249.
100. Kisselburgh LG, Hess J, Zoltowski C, Beever J, Brightman AO (2016) Assessing a scaffolded, interactive, and reflective framework for developing ethical reasoning skills of engineers. In *Proceedings of the 2016 American Society for Engineering Education*, New Orleans.
101. Skirpan, M., N. Beard, S. Bhaduri, C. Fiesler, and T. Yeh. 2018. Ethics education in context: A case study of novel ethics activities for the CS classroom. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*. New York: ACM. https://doi.org/10.1145/3159450.3159573.
102. Warren, S.D., and L.D. Brandeis. 1890. The right to privacy. *Harvard Law Review* 4 (5): 193–220. https://doi.org/10.2307/1321160.