Privacy versus Convenience: A Historical Perspective, Analysis of Risks, and an Informatics Call to Action

Larry Ozeran[1] Anthony Solomonides[2] Richard Schreiber[3]

[1] Clinical Informatics, Inc., Woodland, California, United States
[2] Outcomes Research Network, Research Institute, NorthShore University HealthSystem, Evanston, Illinois, United States
[3] Penn State Health Holy Spirit Medical Center, Information Services, Geisinger Commonwealth School of Medicine, Camp Hill, Pennsylvania, United States

Address for correspondence Richard Schreiber, MD, FACP, FAMIA, Penn State Health Holy Spirit Medical Center, Geisinger Commonwealth School of Medicine, 431 North 21 Street, Suite 101, Camp Hill, PA 17011, United States (e-mail: rschreiber@pennstatehealth.psu.edu).

Appl Clin Inform 2021;12:274–284.

Abstract

Background The pace of technological change dwarfs the pace of social and policy change. This mismatch allows for individual harm from lack of recognition of changes in societal context. The value of privacy has not kept pace with changes in technology over time; individuals seem to discount how loss of privacy can lead to directed personal harm.

Objective The authors examined individuals sharing personal data with mobile health applications (mHealth apps) and compared the current digital context to the historical context of harm. The authors make recommendations to informatics professionals to support consumers who wish to use mHealth apps in a manner that balances convenience with personal privacy to reduce the risk of harm.

Methods A literature search focused by a historical perspective of risk of harm was performed throughout the development of this paper. Two case studies highlight questions a consumer might ask to assess the risk of harm posed by mobile health applications.

Results A historical review provides the context for the collective human experience of harm. We then encapsulate current perceptions and views of privacy and list potential risks created by insufficient attention to privacy management.

Discussion The results provide a historical context for individuals to view the risk of harm and shed light on potential emotional, reputational, economic, and physical harms that can result from naïve use of mHealth apps. We formulate implications for clinical informaticists.

Conclusion Concepts of both harm and privacy have changed substantially over the past 20 years. Technology provides methods to invade privacy and cause harm unimaginable a few decades ago. Only recently have the consequences become clearer. The current regulatory framework is extremely limited. Given the risks of harm and limited awareness, we call upon informatics professionals to support more privacy education and protections and increase mHealth transparency about data usage.

Keywords
- privacy
- security
- mHealth apps
- consumer health informatics

received
October 16, 2020
accepted after revision
February 24, 2021

Georg Thieme Verlag KG,
Rüdigerstraße 14,
70469 Stuttgart, Germany

DOI https://doi.org/10.1055/s-0041-1727197.
ISSN 1869-0327.

Background and Significance

The pace of technological change outstrips the pace of social and policy change,[1,2] and we observe that consumer-directed mobile health applications (mHealth apps—both phone apps and browser based) are ubiquitous.[3] Concerns emerged about the risks of unforeseen or unexpected uses of personal data[4,5] long before the more recent questions about COVID-19 tracing and tracking, and to be clear, the focus in this paper is on *freely shared data*, not on breaches or theft. The concern is with the harm that can result from the uncritical willingness to share personal data with an mHealth app (and its developer) to receive certain services.

Concerns about technology and its impact on the human sphere are not new. In 1964, with the United States embarking on its greatest scientific adventure, and with the United Kingdom experiencing "the white heat of technological revolution," Lewis Mumford[6] lamented the loss of human autonomy: "Why has our age surrendered so easily to the controllers, the manipulators, the conditioners of authoritarian techniques? The answer to this question is both paradoxical and ironic." He goes on to observe that economic persuasion is more effective than coercion: all are promised a share in the new prosperity. If we translate this reflection in terms of information rather than material goods, we recognize an echo in the digital era that has brought with it instant connectivity and access to vast volumes of information at the cost of loss of privacy.

Reflection on the issues raised by ubiquitous technology and massive data collection on a historically unprecedented scale raises more questions than it answers.[7] The lament at the loss of privacy at one end competes for space—in physical and online magazines, in blogs, in comments columns—with the opposite view, reflected in the perspectives "you only get the privacy you fight to keep" contrasted with "there is no privacy, get used to it."[8] The Google ad for women's running shoes that follows a search for trainers for a spouse is the reminder that something automatic is going on in the background: we are being watched.

Why does this appear tolerable? The study of "information commons"—counter to the dismal spirit of Garret Hardin's "Tragedy of the Commons"—led Elinor Ostrom and colleagues[9,10] to analyze commons in terms of *subtractability* and *exclusion*. Certain common goods are subtractable, in the sense that enjoyment by one party reduces or eliminates the opportunity for others equally to enjoy those goods; a clear example would be a monograph published in limited numbers (where subtraction, once the print run is exhausted, is total) or books in a library (where subtraction is temporary—others will enjoy the book once it is returned). Exclusion relates mainly to the means one may obtain access to a good: is it freely available, or does it carry a price tag or require a subscription? The cost of access calibrates the degree of exclusion. For the most part, information on the Internet appears to suffer from no subtractability at all, and a relatively small fraction of it is subject to exclusion behind a paywall. It seems plausible that the ubiquity and richness of information on the Internet have led to a radical discounting of the value of that information. Google and Facebook have succeeded in their efforts to collect, collate, and sell the highly personal information of their users largely by labeling the data collected as "digital exhaust."[11] While intentionally implying that this information would otherwise be wasted, the data are highly valued once organized and supplemented with data collected from multiple other sources. Thus, the trade-off between privacy and convenience happens not only in the instant of use, the moment when some nugget of information appears worth divulging name, birth date, or mobile number, but also more largely in the culture as a whole. Technology companies publicly devalue personal information to make it appear that we gain much more than we surrender,[12] while telling investors the opposite.[7]

mHealth apps in domains as diverse as weight management, bipolar disorder, HIV protection, and care of the elderly have focused on the value of the app and its convenience for the user, but not on the potential loss of privacy and risk of related harm.[13–16] Several studies have observed that mHealth apps often have poor or no privacy protection.[17–20] The potential value of collected data is emphasized by "… three ways in which self-trackers attribute meaning to their data-gathering practices which escape this data fetishist critique: self-tracking as a practice of mindfulness, as a means of resistance against social norms, and as a communicative and narrative aid."[21] Here data fetishism is defined as the conversion of data to economic value.

Objective

The authors' goal is to raise awareness of and knowledge about the risk of harm from indiscriminately sharing personal information with mHealth apps and to recommend that informatics professionals ought to support consumers, both directly and through clinical colleagues, to better balance convenience with privacy while using mHealth apps. We present a historical context for human understanding of harm that helps to demonstrate why consumers discount the risks of harm. We then detail the risks of harm that users of mobile health applications face as these apps have become ubiquitous and incorporated into modern health care.

Methods

The authors performed several literature searches (see ►Appendix A). The first used PubMed through December 31, 2019 and included e-pub ahead of print, in-process, and Medline Daily. This retrieved 19 articles. The second query was a modification of the first. The third included broader MeSH terms. These were performed on December 3, 2020. The goal of the searches was to find current and historical articles that considered the intersection of privacy issues and consumer-oriented mobile or mHealth applications. Exclusion criteria included telehealth or telemedicine, medical monitoring applications such as those for blood glucose, or

Table 1 Results of search queries

Query	Articles retrieved	Reason for exclusion	Excluded	Articles remaining
1	19		0	19
2 (1980–2021)	10,323			10,323
		Telehealth/telemedicine	6,487	
		Application risks	2,497	
		Not consumer oriented	1,229	
		Used for monitoring	21	
		Regulatory	1	
		Not pertinent	68	
		Duplicate from prior query	2	
		Total excluded		10,290
	Deemed highly relevant by authors			**18**
3 (1980–2021)	1,119			1,119
(1986–2021)		Not policy oriented	886	
		Not pertinent	193	
		Duplicate from prior query	7	
				1,086
	Deemed highly relevant by authors			**33**
Total articles for initial review				**70**

those prescribed by a physician, or applications for use in home monitoring such as post-hospital discharge. The intent of this paper is to focus on the willful sharing of one's own personal data, not to discuss access or authentication integrity, or security issues such as hacking, device or application vulnerabilities, or data integrity. One of us (R.S.) reviewed all the titles of retrieved articles to winnow down the total. ►**Table 1** summarizes the results of this process.

The authors also explored the references in these articles and "similar articles" as suggested by PubMed for appropriateness. All authors performed individual article searches and pursued references independently to find diverse sources of evidence and opinion including references from the original articles, studies known to the authors, consultations with experts who recommended other articles, recent news items, internet blog posts, significant media stories, and reviews, as well as academic articles from nonhealth domains (e.g., law, ethics).

The literature search included reviews which afforded the opportunity to view how the risk of harm has changed slowly over long periods of time, and to observe trends that may suggest mitigation for the identified risks potentially available to users.

The authors convened frequently to discuss current findings, reassess the direction of the research, and develop a consensus on the direction of the investigation and analysis.

Case Studies

Of thousands of mHealth apps, only some of which have solid privacy protections, we present two case studies to illustrate our focus that consumers need to recognize that an mHealth app may pose risks of harm that might not otherwise be considered plausible. For example, would one predict that by sharing fertility data with an mHealth app that the user could be stalked due to the developer's terms of service? Without such an example, that might be considered hyperbole or unrealistic conjecture.

Glow, a Fertility App

Physicians and other clinicians are encouraging patients to participate more in their care by using mobile health (mHealth) apps, such as pregnant+for women with gestational diabetes.[22] At the same time, third parties, including pharmaceutical companies, may approach these app developers to buy personal data. Are users aware of the sale of their data? How do they feel about this? What are the risks of harm to individuals?

An article by the Daily Beast describes the fertility app "Glow" as "a Jackpot for Stalkers."[23] In it they said,

> The pregnancy and period app Glow unwittingly exposed women's health information to anyone who wanted to look…

> Every day, female users are encouraged to upload their body temperature, sex drive, alcohol intake, sexual activity, cervix position, and more. They can cross-reference their data with male partners, who are encouraged to dutifully upload intimate information like their masturbation habits. Users who crave even more feedback can take their questions to supposedly anonymous Glow forums, where people seek advice on everything from sex positions to dealing with the aftermath of rape.

The article brought to light several important concerns. Glow linked a woman's account to the first man who asked. The woman could not block the connection if she was not already linked to someone else. Could the first time this security limitation is recognized be when a stalker uses the Glow information to harm someone?

The Daily Beast post[23] also accused another app, "Menstrual Period Tracker," of selling data, a claim the company denies.

Glow's privacy policy[24] should raise concern. In addition to the very sensitive personal information collected from users, they also collect additional health information using links to services like Apple HealthKit and Google Fit. Glow collects and retains payment information. They explicitly state that they can keep a user's information even after use of the service ends:

> You authorize Glow to use all such data, including data that may relate to HIV and/or other sexually transmitted diseases, mental and behavioral health conditions and treatment, substance abuse conditions and treatment, and other sensitive data, throughout the term of your use of the Services, to store such data as described herein, and to store and use it as described in this policy or that agreement **even once you are no longer using the service** (emphasis added).

A user can stop the collection of data after revoking authorization, but the agreement states that Glow can keep all data obtained prior to the revocation.

This is not intended to serve as an indictment of Glow specifically, but rather as an example of the risks individuals face in ways that they might not have considered in the absence of a concerted effort to educate them and promote transparency of data usage.

COVID-19 Tracking Applications

The California Department of Public Health (CDPH) has encouraged the public to enroll in an application to receive an alert if users encounter a person known to be COVID-19 positive.[25] Users of Android devices must download an application, whereas for iOS there is no application, rather a change in settings. The privacy policies are available on the website; the laws and public policies on which the app is based include HIPAA. There is explicit information regarding what information is and is not collected; all data auto-deletes after 14 days; any data the state collects is de-identified; and there is a clear declaration that the CDPH will not disclose any personal information without the individual's consent. There is information about how to contact the CDPH privacy officer by mail or email. The entire privacy policy is on a single, brief web page. However, the content is at an advanced reading level (Flesch-Kincaid level 17.5, Microsoft Word, Redmond, Washington). There is no mention of third-party companies, not even the app developer, nor if they have a relationship with the notification service or the application.

Pennsylvania has made the same application available, but the privacy notice for the Pennsylvania "Exposure Notification System" is more difficult to find on the web.[26] It is more readily available when one downloads the app. In contrast to the CDPH version, the Pennsylvania policy is far more detailed but reads at a Flesch-Kincaid level of 9.5. There are no manifest contradictions between the two policies, but each mentions items not found in the other. Thus it is possible for residents of different states to get different privacy information even when using the same mHealth application.

These variations in policy will have different implications in determining the risk of harm to the individual and make it harder for a consumer to perform a critical assessment. While not a firm conclusion, this raises the question of whether privacy policies need to have some standard for consistency and reading level. In particular, when two entities use the same third party mHealth app, should consumers get the same privacy notice, modified only by underlying jurisdictional differences?

Reflections Regarding the Case Studies

These case studies raise several questions:

- What is the balance between privacy and convenience and what should it be?
- What privacy protections should users expect when using an mHealth app?
- How can users of an mHealth app know if they are exposing private information?
- How may the data be shared and who might see the data that a user enters or the aggregated data after integration with additional datasets?
- What are the economic and noneconomic costs, including risks of harm, of entering personal data?
- What can users do to mitigate the risks of using an mHealth app?

Results

Historical Context of Harm

It has long been observed that technical change is faster than and often drives social change, while changes in policy to provide guardrails to reduce the harm of these changes occur late in the social transition.[27] As such, it is important to provide some context to the pace of change, to appreciate why we are here, why we have not intentionally and explicitly managed the balance of privacy versus convenience in consideration of the risk of harm.[27,28] It is also important to understand how historically a consumer confronted by the

proverbial "man with a gun" sees an imminent risk, but the relative newness of mHealth apps does not present this same obvious danger.

We identify four domains of harm: emotional, reputational, economic, and physical. For each of these, in different ways, physical distance and means of access play a part. We contend that a sense of distance, more precisely of remoteness and anonymity,[29] contributes at a subliminal level to the sense of safety that allows people to be so comfortable just sharing data with no context that there even could be harm from simply sharing data. We outline several strands in the history of technology as a means of causing harm. The categories selected were intended to highlight changes in the mechanisms of causing physical harm (Communication—Information and Images; Transportation; Methods of Physical Harm) and emotional or reputational harm (Norms of Politeness and Discretion). Transportation also impacts financial harm in terms of the traditional view of theft. The time periods in ►Tables 2 and 3 were selected to show how the ability to cause harm more rapidly and at lower cost has increased over time, gradually at first, but extremely rapidly in the past 20 years.

These periods represent pivotal times in United States or world history: the United States Declaration of Independence in 1776; the end of the American Civil war in 1865; the early 1900s provide watershed moments in science and scientific technology; they are followed by a half-century of two world wars and very rapid scientific progress, culminating in nuclear weapons and a period of economic reconstruction, symbolized here by 1955; by the end of the 20th century, reconstruction had given way to globalization, bringing in its wake the modern technologies that are of central concern in this paper. Listings within each cell are meant in some sense to graduate from those issues most proximal to the individual to those most distal.

In our digital world, it is now possible to harm someone instantly by word and image on social media (emotional, reputational, or both), economically by profiling aggregated (health) data, and physically by remote drone. Policy has not kept pace and equally importantly, human awareness has also lagged. In this environment, how do we view privacy today?

Results of Literature Overview

Of the articles which the authors deemed most relevant to study the tension between privacy concerns and convenient use of mHealth apps, it was evident that the research thus far has been fairly narrowly focused. ►Table 4 shows that the most pertinent research covers nine distinct categories, with many recent articles concerned with the COVID-19 pandemic.

Table 2 Changing human experience over time—independence to Post World War II

Domain Year	Means of communication	Images	Transportation	Methods of physical harm	Social norms of politeness and discretion
1776[45]	Person-to-person Messenger Newsletter Newspaper	Hand-drawn sketches Diagrams Paintings	Horse-drawn carriages Rough roads Boats on rivers or coastal waters Long-distance travel both a luxury and a hardship	Small arms and other personal weapons Usable within a small range of the victim 1791: "… the right of the people to keep and bear arms, shall not be infringed"	Core values: discretion privacy vs. disclosure ill-health not discussed Physicians withhold fatal prognosis Contrast: personal attacks in pamphlets[46]
1865	Telegraph introduced Meaningful messages transmitted quickly over large distances	Professional craft of black and white photography	Trains Incompatible gauge tracks Seafaring a comfortable luxury	More accurate rifles with greater range Smith and Wesson revolvers already in use	Regional differences in degrees of politeness and discretion Radical political differences dominate
1900	Telephones through manual exchanges First payphones	1888 George Eastman's first consumer camera 1900: "Brownie" box camera Cinema first movies Public events as news	Automobiles[47] Tarmac road surface[48] First paid flights begin in 1914[49] Government legislation Accidents and real harms motivate new laws	Automatic rifles, pistols 1904: "Luger" pistol Browning automatic rifle deployed in World War I	1890: "Right to privacy" (Warren and Brandeis)[50] Unapproved portraiture is a legal injury
1955	Radio and TV main carriers of news Automatic phone exchanges Direct long-distance calls "Phreaks" hack telephones Mainframes "Data processing" Storage on tape, disk	Color photography Periodicals popular SLR cameras Earth photographed from space 1957: Brownie with flash 1963: Kodak instamatic	Economic growth Motor vehicle numbers Interstate highway program 1970: 50% of U.S. households have a car[51] Truck numbers grow fast	Personal firearms and automatic weapon symbolic among subcultures (e.g., survivalist cults)	The "American Family" dominates public values in U.S Segregation challenged The contraceptive pill and women's liberation Satire targets scandals and misdeeds by public figures

Table 3 Changing human experience over time—the 21st century

Domain Year	Means of communication	Images	Transportation	Methods of physical harm	Social norms of politeness and discretion
2000	Brick-sized "mobile" devices give way to smaller cellular phones[52] Printers, copiers, fax machines integrate into multifunctional devices Networked mini- and personal computers common[53] email (with attachments) becomes an accepted medium of communication[54] Hacking makes its earliest mark	Nature documentaries exploit high quality color television to display natural wonders Hubble telescope and other space missions send back astonishing images of the cosmos	Despite concerns about environmental impact, air travel has proven so popular that "budget" airlines launch profitable services to and from less prominent destinations The car appears less popular, but roads are busy and poorly maintained Since 1997, truck sales exceed those of automobiles	Gun crime has increased, often in the wake of drug wars and street gangs Of the 27 mass-shooting incidents in the United States in the last decade of the 20th century, 13 took place in 1997–1999, six in 1999 alone	Backlash to social and sexual freedoms won over past 25 y is accentuated by an HIV/AIDS epidemic that makes a convenient target for social conservative Rapid communications make political scandals and revelations common, with popular cynicism to match Liberalization of markets in the 1990s creates new social classes with marked movement away from communitarian values
2020	At this stage little sense in separating communications from images It seems McLuhan's dictum, "The Medium is the Message," has come to pass The mature cellphone, or smartphone, is now a veritable media center[54] Permits audio and video communication, including video of police carrying out arrests or other duties, sometimes with bad consequences Possible to listen to music, read a book, schedule appointments, and so on Also, possible to upload photos of oneself and one's surroundings or companions instantly to a popular sharing "app," so that a distant cousin in another country can see what you are doing almost as soon as you have done it "Cyberbullying," "sexting," and "revenge porn" have all become common terms in discussing the dangers of a "hyperconnected" society Violent video gaming suspected of encouraging violence With the COVID-19 pandemic making face-to-face meetings or even visits to friends difficult, video communication apps have been adopted to an extraordinary degree		Automobiles have become luxury environments, often offering the most comfortable seating and best audio sound available to the owner Air travel has been dented by the COVID-19 pandemic, but travel by car has substituted for some, with people choosing to drive significantly longer distances	General perception of increased violence is in part contradicted by statistics Vigilante violence appears to have been exacerbated by political polarization Guns and gun modifications (e.g., bumper stocks) have become ever more sophisticated For those with the power and resources, it is now possible to explode a person thousands of miles away without leaving home[55] Possible to capture,[30] alter,[31] and publish unwitting photographs of individuals in compromised situations	Increasingly self-revelatory culture, both in the media representation of "celebrities" and at a personal level in popular apps, such as Facebook Attitudes are expressed in resigned phrases, such as "there is no privacy," or "you have to move with the times" A trend to substitute "end-user license agreements" (EULAs) for informed consent

A major finding of this literature review is the scarcity of academic literature regarding the risks of harm from willingly sharing personal data with third party health applications. The authors find it remarkable that in the past 10 years or so there are only 70 applicable studies, of which half explore general policies and not specific risks. In the past 1 year, 10% of the articles discovered involve the SARS-CoV-19 (severe acute respiratory syndrome coronavirus 2) epidemic and mHealth apps regarding the pandemic. This despite numerous reports in the popular and gray literature, some of which are cited here,[23,24,30–32] regarding privacy risks.

Current Views of Privacy

According to the Pew Research Center, "Most Americans see privacy issues in commercial settings as contingent and context-dependent."[32] People weigh the deal being offered, how much they trust the company, and their life circumstances when deciding whether to share personal information or permit surveillance.[33] In this 2015 Pew survey, people supported accessing one's medical records and making appointments at the doctor's office more than five other scenarios (none health related). The survey authors question, but do not explore, whether each person has enough information about the real costs of exposing their information to make an informed decision. For example, people know not to share their social security number (which can be changed if misused) yet seem content to share their birth date (which is immutable). There is an opportunity to educate about both risks and methods to mitigate harm.

The Pew study[32] also found that 91% of Americans "agree" or "strongly agree" that people have lost control over how personal information is collected and used by all kinds of entities. Most social media users are concerned about advertisers and businesses accessing the data they share on social media platforms and want the government to regulate advertisers. Over 60% want more done to protect privacy.

Elderly individuals with chronic illness may be willing to share health information with their children but maintain control of decision making.[34] People who are ill tend to be more willing to share their health data than people who are well.[35]

Table 4 Topic categories of current research on privacy concerns of mHealth applications

Topic area	Number
General policy	45
COVID-19	7
Mental health and related	6
Women's health and sexual health	3
Cancer	2
Children	2
Diabetes	2
Dementia and neurological ailments	2
Social responsibility and digital surveillance	1
Total	70

Frameworks such as the Creating Access to Real-time Information Now through Consumer-Directed Exchange (CARIN) Code of Conduct[36] provide industry guidance. CARIN offers a comprehensive Privacy Impact Assessment tool for ethical and socially responsible design of mHealth apps, including easily understood consequences, such as whether personal data are shared with or sold to third parties. Enhancing transparency of data usage would allow consumers to make safer choices. For example, knowing that an mHealth app sells data to third parties, such as insurance companies, might impact what data are shared by the individual. Might the data be used to deny health care services? Absent education to consider the risk, would consumers be fully informed when using the app? In the light of the Glow case study, what policies do the developer have in place that might lead to harm?

Discussion

mHealth apps have introduced new reasons to assess the risks of trading privacy for convenience. Our historical perspective reveals one facet of the slowly changing context of harm; the literature review another; and the case examples reveal yet a third aspect.

There is little empiric research regarding harm from mHealth apps in the context of trading privacy for the convenience of achieving a user's goals. Of the initial finding of over 10,000 articles meeting our search criteria, the vast majority were not relevant to the research question. Although there has been ample discussion in the media, on blogs, and in the daily news—especially when there have been breaches or revelations of bias or undesirable information sharing—our query only found a few dozen articles that the authors deemed highly relevant to harm from willful data sharing. Unsurprisingly, more than one-half of the articles examined general policies regarding privacy. The recent COVID-19 pandemic has sparked renewed interest in applications dedicated to a specific disease and thus articles regarding this specific topic were numerous. The literature review revealed only a few articles regarding a smattering of other specific diseases or issues. We infer that low volume of privacy articles implies little empiric evidence about protections a user can invoke to protect their identity and personal information. The General Data Protection Regulations[37] certainly establish a high bar regarding regulatory expectations, but these do not apply universally, and are not specific for mHealth apps.

Prior to the internet, social media, and ubiquitous computing, users of communication devices knew with whom they were communicating or were aware of the privacy limitations of the tool they were using. As the historical tables make clear, until the late 20th century privacy was a largely local matter. One did not share information in one medium without being aware that the information could appear elsewhere (barring spying or other devious methods—the equivalent of spyware, malicious software, or computer security flaws not considered in this paper). Current communication and information tools are distinctly different: third-party sharing, tracking cookies, and other hidden manipulations make it difficult if not impossible for new or uninformed users to be aware of the extent to which their data are distributed. The impact of blocking cookies, disabling scripts, and other protective efforts may not be widely known, but even if known, would they reduce the convenience to use the app to a point where they would not be implemented? Do we need simpler data use agreements that follow the CARIN format?

The case studies represent examples of the highly variable privacy protections available to end-users. The Glow application does reveal its privacy policies but given the sensitive nature of the information a woman may share on the application, and that few users take the time to read the end-user license agreement, the application puts that information at undesirable risk. The applications which help to track exposure to, and symptoms of COVID-19 seem to maintain a user's privacy, but it is intriguing that at least two states which use the same software application reveal different aspects of the privacy specifics of that application. It is no surprise that *caveat emptor* (let the buyer beware) still applies after almost 500 years.[38]

Given the risk of harm that can come from sharing health data in certain ways (e.g., with health plans or stalkers), it is imperative to identify ways to enhance the protection of privacy and provide individuals with a better understanding about how to control use of their data by the third parties to reduce the risk of individual harm.[39] Current law becomes increasingly inadequate, obsolete, and fragmented with the advancement of technology.[39] We advocate for consumer education coupled with guidelines consonant with these principles and similar to the CARIN Alliance guidelines to support the needs of mHealth consumers.

Consequences for Informatics

What are the implications of this analysis on informatics professionals? As experts of information storage, retrieval, analysis, sharing, and the accompanying privacy, ethical, and legal issues surrounding personal and other information, we

argue that, at a minimum, informaticists individually and through professional associations should pursue research and initiate debates to:

- Establish public standards for the collection, processing, storage, and sharing of personal data, with clarity as to purpose, responsibility to the data source, and transparency about how revenue that is generated is shared with the source of the data.[14,40–42]
- Clarify rules of persistence, consent, and elimination of the data at the user's option, akin to GDPR rules.[37]
- Enable ease of sharing of data, where permitted, by the use of readily adaptable standards such as FHIR, and a secure server that enables protection of privacy.[43]
- Articulate options for clear privacy policies for the use of mHealth apps.
- Support ease of understanding of these privacy policies, e.g., using automated methods to extract deeply embedded implications or promoting privacy practice standards and implementation guides.
- Promote appropriate protections such as more rigorous encoding and concealment of personal data,[44] and education for consumers.

Conclusion

Concepts of privacy and related risks of harm have changed slowly over decades, even as technological advances have accelerated over the past 20 years. In many ways, technology has provided methods to invade privacy that were unimaginable as recently as a few decades ago. This rapid shift has consequences for consumers and information technology developers which is being recognized only now. The current regulatory framework is extremely limited. It is thus incumbent on consumers to recognize risks they may be taking when using mHealth apps, and a challenge for informatics professionals to provide the means for consumers to recognize and understand these risks. Consumers should be given the education and tools that will allow them to make informed choices about when to share very personal information with mHealth apps so that they may minimize their risk of personal harm. Regulatory authorities should require mHealth apps to be more transparent in how data are shared.

Clinical Relevance Statement

Clinicians are increasingly encouraged to prescribe apps as part of therapeutic regimens in numerous domains, from weight and diet management to pregnancy and mental health. Clinical informaticists must help inform their clinical colleagues of the risks of individual harm that users of mHealth apps are taking when they download the application, insert personal data, and upload those data to the internet, including to their health care providers, and why those risks matter. Clinicians should be positioned to inform their patients about the risks as well as benefits of mHealth apps when prescribing digital therapies.

Multiple Choice Questions

1. The HIPAA privacy and security rules only apply to covered entities and not to third-party mHealth applications. What is the best advice an informaticist can offer to an individual to minimize risk of harm when using a third-party application even if it is connected via an application programing interface (API) to a covered entity through the electronic health record?
   a. To access the "designated record set" which includes items "disseminated by a covered entity."
   b. To ask a covered entity to reveal to whom the covered entity sent personal health information.
   c. That individuals have the right and can ask to see and receive copies of their medical records.
   d. To review the privacy statements and policy of the application and use it only if reasonable.

   Correct Answer: Option d is the best correct answer. Although a, b, and c are all valid, they do not offer any privacy protection regarding the third-party application. There are no guarantees regarding the actions of the third party, as they are not covered entities and HIPAA rules do not apply to them. It is up to the individual to determine if they are comfortable with the privacy policies of the application.

2. This article mentions the CARIN Code of Conduct Comprehensive Privacy Impact Assessment tool. This tool makes recommendations for:
   a. Consumer guidelines for safe selection of mHealth apps.
   b. Ethical and socially responsible design of mHealth apps.
   c. Guidelines for safely choosing mHealth apps.
   d. Governmental regulations for designing mHealth apps.

   Correct Answer: Option b is correct. This paper discusses the aspects in the other answers, but only b is correct.

Author Contributions

L.O. conceptualized this paper and initiated the project. All three authors contributed equally to the research, wrote and edited the paper, and approved it for final submission.

Protection of Human and Animal Subjects

No research was performed on human subjects, and no personal health information was obtained, thus institutional review board review was not required.

Supplementary Material

Readers may find details of the search queries in ►**Appendix A**.

Funding

None.

Conflict of Interest

None declared.

Acknowledgments

The authors wish to thank members of the Ethical, Legal, and Social Issues Working Group of the American Medical Informatics Association, and especially the following colleagues who provided insight, support, suggestions, and published works to inform and support the initial direction of this project: Bonnie Kaplan, Marge Benham-Hutchins, Eric Pan, Carolyn Petersen, and Vignesh Subbian.

For assistance with PubMed searches we thank Edie Asbury at Penn State Health Holy Spirit Medical Center.

References

1 Morison EE. Men, Machines and Modern Times. New York: New American Library; A Mentor Book; 1977
2 Morison EE. From Know-How to Nowhere: The Development of American Technology. New York: Basic Books, Inc.; 1974
3 Adams S. Ubiquitous digital devices and health: reflections on Foucault's notion of the clinic. In: Adams S, Purtova N, Leenes R, eds. Under Observation: The Interplay Between eHealth and Surveillance. Law, Governance, and Technology Series. Vol 35 Cham: Springer; 2017
4 Kennedy M. Equifax says 2.4 million more people were impacted by huge 2017 breach. March 1, 2018. Accessed February 23, 2021 at: https://www.npr.org/sections/thetwo-way/2018/03/01/589854759/equifax-says-2-4-million-more-people-were-impacted-by-huge-2017-breach
5 Murphy M. A new data breach may have exposed personal information of almost every American adult. MarketWatch June 28, 2018. Accessed February 23, 2021 at: https://www.marketwatch.com/story/a-new-data-breach-may-have-exposed-personal-information-of-almost-every-american-adult-2018-06-27
6 Mumford L. Authoritarian and democratic technics. Technol Cult 1964;5(01):1–8
7 Lyall B. Fitness for sale: the value of self-tracking in secondhand exchange. Inf Soc 2019;35(03):109–121
8 Geist M. Canada Research Chair in Internet and E-commerce Law, University of Ottawa. The Internet: Do We Really Have No Privacy and Should We Just Get Over It? November 4, 2014. Accessed February 23, 2021 at: https://www.youtube.com/watch?v=DauecZ6Ja_Q
9 Ostrom E, Gardner R, Walker J. Rules, Games, and Common-Pool Resources. Ann Arbor, MI: University of Michigan Press; 1994
10 Hess C, Ostrom E, eds. Understanding Knowledge As Commons. From Theory to Practice Cambridge, MA: MIT Press; 2011
11 Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs; 2019
12 Webb A. The Big Nine: How the Tech Titans and Their Thinking Machines Could Warp Humanity. New York, NY: Public Affairs; 2019
13 Holzmann SL, Holzapfel C. A scientific overview of smartphone applications and electronic devices for weight management in adults. J Pers Med 2019;9(02):E31
14 Nicholas J, Larsen ME, Proudfoot J, Christensen H. Mobile apps for bipolar disorder: a systematic review of features and content quality. J Med Internet Res 2015;17(08):e198
15 Goldenberg T, McDougal SJ, Sullivan PS, Stekler JD, Stephenson R. Preferences for a mobile HIV prevention app for men who have sex with men. JMIR Mhealth Uhealth 2014;2(04):e47
16 Anthony Berauk VL, Murugiah MK, Soh YC, Chuan Sheng Y, Wong TW, Ming LC. Mobile health applications for caring of older people: review and comparison. Ther Innov Regul Sci 2018;52(03):374–382
17 Grundy Q, Chiu K, Bero L. Commercialization of user data by developers of medicines-related apps: a content analysis. J Gen Intern Med 2019;34(12):2833–2841
18 Sunyaev A, Dehling T, Taylor PL, Mandl KD. Availability and quality of mobile health app privacy policies. J Am Med Inform Assoc 2015;22(e1):e28–e33
19 Dehling T, Gao F, Schneider S, Sunyaev A. Exploring the far side of mobile health: information security and privacy of mobile health apps on iOS and Android. JMIR Mhealth Uhealth 2015;3(01):e8
20 Zhou L, Parmanto B, Alfikri Z, Bao J. A mobile app for assisting users to make informed selections in security settings for protecting personal health data: development and feasibility study. JMIR Mhealth Uhealth 2018;6(12):e11210
21 Sharon T, Zandbergen D. From data fetishism to quantifying selves: self-tracking practices and the other values of data. New Media Soc 2017;19(11):1695–1709
22 Garnweidner-Holme L, Hoel Andersen T, Sando MW, Noll J, Lukasse M. Health care professionals' attitudes toward, and experiences of using, a culture-sensitive smartphone app for women with gestational diabetes mellitus: qualitative study. JMIR Mhealth Uhealth 2018;6(05):e123
23 Weill K. This fertility app is a jackpot for stalkers. Updated April 13, 2017. Accessed February 23, 2021 at: https://www.thedailybeast.com/this-fertility-app-is-a-jackpot-for-stalkers
24 Glow Privacy Policy. Updated March 31, 2020. Accessed February 23, 2021 at: https://glowing.com/privacy
25 Privacy Policy. California Department of Public Health. Accessed February 23, 2021 at: https://www.cdph.ca.gov/Pages/privacy-policy.aspx
26 Covid Alert Data and Privacy. Pennsylvania Department of Health. Accessed February 23, 2021 at: https://www.health.pa.gov/topics/disease/coronavirus/Pages/COVID-Alert-Data.aspx
27 Enriquez J. Right/Wrong: How Technology Transforms Our Ethics. Cambridge, MA: MIT Press; 2020
28 Catalog of Problematic Data Actions and Problems. NIST Privacy Risk Assessment Methodology (PRAM) package. Accessed February 23, 2021 at: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/resources
29 Regner T, Riener G. Privacy is precious: on the attempt to lift anonymity on the internet to increase revenue. J Econ Manage Strategy 2017;26(02):318–336
30 Stack L, Holson LM. Katie Hill gives farewell speech to congress, denouncing 'gutter politics.' Accessed February 23, 2021 at: https://www.nytimes.com/2019/10/31/us/politics/katie-hill-speech.html
31 Sample I. What are deepfakes—and how can you spot them? The Guardian. January 13, 2020. Accessed February 23, 2021 at: https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them
32 Madden M. Public perceptions of privacy and security in the post-Snowden era. November 12, 2014. Accessed February 23, 2021 at: https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/
33 Rainie L, Duggan M. Privacy and information sharing. January 14, 2016. Accessed February 23, 2021 at: http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/
34 Crotty BH, Walker J, Dierks M, et al. Information sharing preferences of older patients and their families. JAMA Intern Med 2015;175(09):1492–1497
35 Bell EA, Ohno-Machado L, Grando MA. Sharing my health data: a survey of data sharing preferences of healthy individuals. AMIA Annu Symp Proc 2014;2014:1699–1708
36 Anon. Trust framework and code of conduct. The CARIN alliance code of conduct Accessed February 23, 2021 at: https://www.carinalliance.com/our-work/trust-framework-and-code-of-conduct/
37 General Data Protection Regulations. Accessed February 23, 2021 at: https://gdpr-info.eu/

38 Fitzherbert J. The Book of Husbandry. 1523. Reported first use of phrase, as "[The horse] is no chapmans ware yf he be wylde: but and he be tame and haue ben rydden vpon, than caueat emptor, be ware thou byer." Accessed February 23, 2021 at: https://people.howstuffworks.com/caveat-emptor.htm
39 Kaplan B. Selling health data: de-identification, privacy, and speech. Camb Q Healthc Ethics 2015;24(03):256–271
40 Baumel A, Faber K, Mathur N, Kane JM, Muench F. Enlight: a comprehensive quality and therapeutic potential evaluation tool for mobile and web-based ehealth interventions. J Med Internet Res 2017;19(03):e82
41 Zhu G, Liu H, Feng M. An evolutionary game-theoretic approach for assessing privacy protection in mHealth systems. Int J Environ Res Public Health 2018;15(10):E2196
42 Helm J, Jones RM, Jones RM. Practice paper of the academy of nutrition and dietetics: social media and the dietetics practitioner: opportunities, challenges, and best practices. J Acad Nutr Diet 2016;116(11):1825–1835
43 Zhu S, Chen T, Wang Y, Xiao L, Alterovitz G. A FHIR-based PPS system can keep your genes private. Accessed February 23, 2021 at: http://cseweb.ucsd.edu/~shz338/images/PPS_Privacy.pdf
44 Khan S, Abbas N, Nasir M, et al. Steganography-assisted secure localization of smart devices in internet of multimedia things (IoMT). Multimed Tools Appl 2020. Doi: 10.1007/s11042-020-09652-5
45 Wikipedia. Timeline of historic inventions. Accessed February 23, 2021 at: https://en.wikipedia.org/wiki/Timeline_of_historic_inventions
46 Chernow R. Alexander Hamilton. New York: Penguin Press; 2004: 661–664
47 Anon Automobile history A&E Television Networks. History Channel. Accessed February 23, 2021 at: https://www.history.com/topics/inventions/automobiles
48 Geare J. Which was the first paved road in America? Quora. Accessed February 23, 2021 at: https://www.quora.com/Which-was-the-first-paved-road-in-America
49 Anon. History of aviation—first flights. Accessed February 23, 2021 at: https://www.avjobs.com/history/
50 Warren SD, Brandeis LD. The right to privacy. Harv Law Rev 1890; 4(05):193–220
51 White MG. Car ownership statistics. Accessed February 23, 2021 at: https://cars.lovetoknow.com/Car_Ownership_Statistics
52 Goodwin R. The history of mobile phones from 1973 to 2008: The handsets that made it all happen. Accessed February 23, 2021 at: https://www.knowyourmobile.com/nokia/nokia-3310/19848/history-mobile-phones-1973-2008-handsets-made-it-all-happen
53 Wikipedia. Windows 3.1x. Accessed February 23, 2021 at: https://en.wikipedia.org/wiki/Windows_3.1x
54 Smith A. Overview of smartphone adoption. Accessed February 23, 2021 at: http://www.pewinternet.org/2011/07/11/overview-of-smartphone-adoption/
55 BBC News. Qasem Soleimani: US kills top Iranian general in Baghdad air strike. January 3, 2020. Accessed February 23, 2021 at: https://www.bbc.com/news/world-middle-east-50979463

Appendix A

Query 1

SEARCH TERM(S)

*MOBILE APPLICATIONS or *INTERNET or *CELL PHONE or MOBILE (title word) or

WEB (title word) or SMARTPHONE (title word) or APP (title word) or APPS (title word) or TOOL: (title word)

and

*CONFIDENTIALITY or *PRIVACY (including specific types) or CONFIDENTIAL: (title

word) or PRIVACY (title word)

and

*ETHICS (including specific types) or ETHIC: (title word)

or

*MOBILE APPLICATIONS or MOBILE (title word) or APP (title word) or APPS (title word)

and

*ETHICS (including specific types) or ETHIC: (title word)

Query 2

SEARCH TERM(S)

("mobile app*" OR "mobile-based" OR mHealth OR "mobile health app" OR smartphone) AND ((privacy OR risk OR confidential*) OR ethic*)

Then added:

NOT (telehealth OR telemedicine)

Then:

Removed "OR risk"

Then added:

AND consumer

Then added:

NOT monitor*

Query 3

SEARCH TERM(S)

("mobile app*" OR "mobile-based" OR "mHealth" OR "m-health" OR "mobile health app" OR smartphone OR "consumer health informatics" [MeSH] OR consumer health education [MeSH terms]) AND (privacy OR confidential* OR ethic*) NOT ("telehealth" OR "Telemedicine" OR hospital OR office OR clinic)

Limit

1980–2021

Added:

AND policy

and changed limit: 1986–2021

