Proceedings of the 2022 Design of Medical Devices Conference
DMD2022
April 11-14, 2022, Minneapolis, MN, USA

DMD2022-1045

COMMUNICATING CYBERSECURITY AND PRIVACY DESIGN ATTRIBUTES THROUGH PRIVACY LABELING OF CONSUMER ELECTRONIC MEDICAL DEVICES

Monroe J. Molesky
Department of Health Policy and Management
Milken Institute School of Public Health
The George Washington University
Washington, DC, USA

ABSTRACT

The emergence of electronic medical devices has facilitated the integration of cybersecurity and privacy practices into the design of medical devices. An essential part of device design is the communication of the device principles to the consumers and providers that will utilize the device. The purpose of this research was to analyze the importance of health information privacy, propose a medical device privacy label and standards that can help fill these gaps for consumers, and evaluate the regulatory framework for which this proposal can be implemented. Privacy, both physical and informational, is a key pillar of American healthcare especially in our connected worlds. The threat to privacy from criminal actors and the impact that those actions of violating privacy can have on an individual's health are serious. Evaluating previous privacy labels, which lacked in applicability to the healthcare field, this research proposes a unique, standardized consumer privacy label for the FDA to implement, mirroring the design and success of the FDA nutrition label in educating consumers in healthy decision making.

Keywords: Privacy; Device Cybersecurity; FDA; Consumers

1. INTRODUCTION

It is often asserted that healthy citizens are the greatest asset any country can have. The U.S. Food and Drug Administration (FDA) has long been tasked with this major outlook and responsibility of "protecting the public health by ensuring the safety, efficacy, and security" of food, drug, medical devices, and other products [1]. In the ever-modernizing world, these tenants of safety, efficacy, and security are expanding in step with the technological revolutions of their corresponding industries. The medical device industry is one such industry that has seen such significant changes. Today, connected insulin pumps can automatically deliver injections by the touch of a smartphone application, watches can report cardiac rhythms to your physician, elder falls can be detected by accelerometers, and updates can be automatically pushed to implanted pacemakers. As these digital health capabilities grow, there is a new safety and security consideration that is ever present—privacy.

Digital medical devices have grown to have control over consumer physiological processes (e.g. injecting insulin) and have gained access to extensive streams of sensitive health and personally identifiable information (PII). Federal regulators and clinicians have long accepted the principle of privacy as essential to the consumer's relationship with their provider and the care that they receive. However, the focus of consumer privacy in the expanding field of electronic medical devices and connected digital medicine has been lacking. In one report, only 10% of consumers felt that they had control over their personal information with other data representing a lack of consumer trust in both companies and government privacy protections [2]. Consumers face challenges of understanding new technology, learning about the privacy risks of the health devices they use, and the lack of standardization in designing for and communicating these risks. The design of medical devices regarding cybersecurity and privacy principles is just one half of the conversation as these increasingly critical design characteristics must be communicated to device users.

2. APPROACH AND METHODS

2.1 Privacy as Protection of Health

The literature and medical community have long held the critical nature of health information privacy as essential to the healthcare system, patients, and their health. Privacy was core to the medical principles of Hippocrates and since is described as "a core value in healthcare" by the American Medical

Association (AMA) [3]. Breaches of health information privacy are not only philosophically a violation of the bioethics nonmaleficence principle but can cause harm. Research has correlated privacy breaches with social and psychology disruptions because of their impact on such a core and sensitive element of human society. Darhl Pedersen has described that, "to the extent that privacy is being digitally compromised, such crucial psychological functions are being disrupted" [4]. One recent article in the *Journal of Medical Ethics* stated: "clinicians should now advocate a basic right to privacy as a means to safeguard psychological health" [5]. The loss of private health information is a serious concern with the many sensitive aspects of health and there are many examples of medical devices contributing to this risk in their nature and design. For example, researchers at Dartmouth, as part of a National Institute of Drug Abuse study, have developed methods to detect cocaine usage via live heartrate data collected from cardiac enabled medical devices (including smart watches) [6].

Practically, digital medical devices pose a wide set of privacy issues that can affect public health through issues of safety and security. These range from the psychological impacts of breached privacy and stress over consequences (like identity theft) to more physical health concerns like the loss of trust in medical practitioners and direct threats actors using PII. There is a reason why 76.59% of all data breaches (249 million affected individuals) in the last five years have been within healthcare service providers [7]. Health information is considered to be an extremely attractive target for cyber criminals because it contains the most sensitive personal and financial information. This enormous threat of technology to health privacy has been acknowledged by the AMA. The updated AMA Code of Medical Ethics describes that: "respecting patient privacy in other forms is also fundamental, as an expression of respect for patient autonomy and a prerequisite for trust. Patient privacy encompasses a number of aspects, including personal space (physical privacy), [and] personal data (informational privacy)... physicians must seek to protect patient privacy in all settings to the greatest extent possible" [3]. To meet this standard, ways to inform providers and consumers that use digital medical devices of the privacy risks must be developed and standardized.

2.2 Previous Privacy Device Design and Labeling Literature

To approach this issue of privacy communication with electronic devices, there has been a limited exploration of privacy and security "nutrition" style labels. The idea of privacy nutrition labels became popular in 2011 when the U.S. Federal Trade Commission (FTC) suggested the idea. Patrick Kelley at Carnegie Mellon University (CMU) has created the main existing examples of privacy labels and a study by Kelley et al. surveyed over 700 individuals and found that their standardized privacy tables increased the speed of finding the privacy policy specifics, consumer engagement, and accuracy [8,9]. There was 69% accuracy in consumers properly identifying an example label's privacy setting, significantly greater with the label compared to their accuracy reading traditional privacy statements [8]. This label was not well adapted for specific use in the healthcare field with just one category for general health information. A new set of researchers at CMU have updated their label to more closely match the real nutrition label and create a dedicated column for physiological security and privacy information. However, their label still lacks in specifics privacy concerns that are unique to medical devices in practice and the labeling guidelines provided by CMU only twice mentioned their health information column.

Beyond the work at CMU, Apple has taken the greatest advances in their privacy labels on the AppStore. The Apple developed "labels" clearly distinguish health versus fitness data, location tracking, data usage, and disclosing health data that is used in research. However, these labels that are shown on the AppStore still are more focused on the specific features of Apple products and do not go into detail about each category. For example, Apple specifies health and fitness data categories but does not describe if a health data app is only collecting heart rate data or more sensitive PII from your device [10]. While overall data usage is described by category, such as for third-party advertising or product personalization, Apple labels to do not provide much detail regarding how each physiological data stream is utilized. The heart rate data may be used for device product personalization while the health app conducts third-party data tracking that targets your history of attending certain health clinics—both fall into the same label categorization due to the specific focus on health information in this label iteration.

Furthermore, researchers at the firm of Clever°Franke, a Dutch design firm, created a privacy labeling system as part of the European Design Awards competition. Their system focused on a letter grading system of A through F with concentric rings that represented 15 sub-categories of privacy classifications [11]. The simplified design was described as an "easily summarized solution that clearly communicates how organizations deal with our privacy and data ownership and that functions in the physical and digital world" [11]. While their design for ring grading system is unique and they continue to advocate for label adoption in the Netherlands, there is a balance of design, functionality, simplicity, and specificity that the literature shows is needed.

Reviewing the literature, it is clear that the process of privacy labeling is being attempted, but the existing literature on privacy labels is quite limited and has not directly addressed unique privacy concerns and designs related to health information and medical devices. There are three main concerns and gaps in the current labels observed from the literature: 1) lack of specificity of categories characterizing health information privacy; 2) overcomplications of labels for the consumer/provider engagement; and 3) simplifications into broad categories that mottle information sharing.

Examining the existing examples, it is evident that communicating privacy is an essential part of the continuing digitization of healthcare. Healthcare information is some of the most sensitive information an individual retains, and medicine has long been imbued with the importance of privacy—both physical and information privacy. These principles need to be retained in consideration of electronic medical devices while

providing autonomy to consumers to understand and make decisions regarding their health privacy with these devices.

2.3 Design of Device Privacy Labels

The method of design of the privacy label was a several step process of development. First, the above literature examples of existing privacy labels were examined for a commonality in categories and attributes that were described. Of these, there was a common design of identifying what characteristics were simply engaged in that individual project, like with a check mark, and then a descriptive measure of data utilization/sharing. These aspects spoke to key principles of data privacy that informed the consumer what information was being collected and how that information was being used by the device and company. Furthermore, there was generally broad categorizations of data collection types to help organize specific features into more consumer-friendly headings. While this is an important aspect for consumer understanding, existing labels were often lacking in categorizations and descriptions important to specific sectors.

Second, for this study's prototype, the categories (data privacy, sensory privacy, communication) that were used for categorization of specifically listed privacy attributes that would be of most concern in an electronic or digital medical device were designed from previous literature and evaluation of current devices privacy, cybersecurity, and data attributes. Utilizing the existing examples, which are limited by their broad characterization of privacy, several applicable categories from the more general labels (such as PII and Wi-Fi™/Bluetooth® connection) were identified for inclusion on the label.

Third, specific label attributes surrounding sensory data that medical devices collect was identified by reading current digital health device literature as discussed below in Section 2.4.

Beyond content identification, the actual design was mirrored off of the current FDA food nutrition label. The single column white and black label that most Americans are very familiar with is a good example of communicating complex information in a clear, uniform, accessible, and concise format. Since many Americans are used to that type of label and would identify that format as something that would contain important health information, it is a reasonable conclusion to model this label prototype after that general design. Especially as existing labels were inhibited by complex designs, size, and ease of use.

2.4 Identification of Physiological Data Concerns

To identify the physiological, or sensory, data measures that would be a privacy concern in a medical device, several FDA medical device sources were reviewed, and author expertise used. In this review, the most common utilization of connected devices was for cardiac evaluations. However, non-cardiac devices frequently were used for chronic disease monitoring which included a variety of activity tracking/accelerator use that is categorized as motion capture technologies. With those aspects, a mixed bag of various life-style health devices had video, audio, and location recording abilities for safety and research capabilities. Also, recent literature on future electronic medical devices emphasized the ability of devices to investigate environmental body conditions—things such as oxygen saturation, blood sugar levels, temperature, and metabolite/blood markers—along with sleep [12]. These types of developing technologies had to be balanced with comprehension and specificity while maintaining the broadness of categories that would allow for uniform application across device types and developing technologies. Seeking to build a privacy label that can continually develop with the broad category of applications that electronic medical devices play, the following six sensory privacy attributes were selected: heart rate/electrocardiogram (ECG), motion capture, audio, video, body environment, and sleep. We sought to better describe aspects of sensory data collection unique to this space to create a functioning medical device privacy label compared to the more general examples.

3. RESULTS AND DISCUSSION

3.1 Prototype Label

The privacy label prototype matches the nature of a traditional nutrition label while communicating several general data privacy attributes and the specific sensory/communication items unique to a medical device. There are three main categories for the label: data privacy, sensory privacy, and communication. Data privacy embodies three items that address general use of the data including geolocation, data storage, and personal information use. The sensory privacy category is the most unique to the medical devices as health specific data measures. Lastly, communication categorizes describe how the device operates within the healthcare community regarding that private health information including aspects of information sharing.

The communication category describes ways in which the sensory and data information is communicated by the device. Classifications of the device's ability to connect to the electronic health record (EHR) or to a healthcare facility speaks to Wide Area Network (WAN) capabilities specific to the healthcare sector and that are an existing concern in the literature. Two classifications of Local Area Network (LAN) and Personal Area Network (PAN) connections describe the device's ability to connect to more localized, consumer networks such as a home WiFi™ networks. The PAN attribute on the label is meant to be a broad category that can encompass wireless PANs, like Bluetooth® or Zigbee™, that are used to locally connect medical devices at the personal level. Lastly, classifications were created for devices that use cellular networks to communicate their collected data, and for device-to-device connection. Device-to-device connection is a classification that this research determined was necessary to speak to a wide category of device capabilities to directly communicate with other immediate devices. Our research concluded that the connection of multiple devices may not be an attribute consumers would consider independently and research on data aggregation concerns led us to include that reportable attribute option on the label.

Overall, the label takes a two-column approach not only what information is being collected but how that information is being used on three different healthcare specific levels. Three classifications have been prescribed for the information usage

column: remains local, provider sharing, and third-party sharing. Remains local indicates that the information is stored locally on the device or that the collected data is used for personalization of the devices only. Provider sharing indicates that the information collected is securely shared directly with a healthcare provider. The third-party sharing indicator describes to the consumer that a third-party has access to that privacy attribute's information.

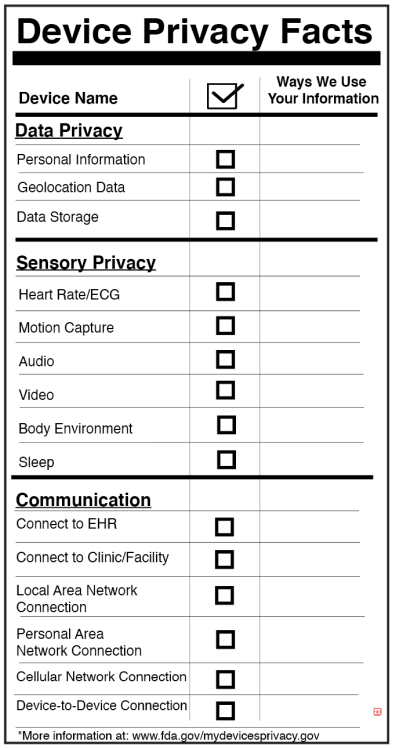

FIGURE 1: BLANK PROTOTYPE PRIVACY LABEL

It is proposed that this device privacy label would appear on electronic medical devices according to 21 CFR Part 801 and Part 830 by displaying the label on the "immediate container of any article" in the "written, printed, or graphic" form as all other medical devices and foods are labeled practically under FDA regulations [14]. The proposed label would be available to consumers upon the packaging of devices. These labels would not be limited to the analog display within packaging materials but have information on the label regarding further electronic resources. Many manufacturers embrace this electronic way for consumers to view product information and the practice is authorized to an extent under Section 2(b)(2)(B)(i) of the Medical Device Technical Corrections Act of 2004.

3.2 Example Device Label

In this case, the below example label in FIGURE 2 is for the G Medical VSMS ECG Patch that has recently been approved by the FDA to remotely monitor the heart and vital conditions of patients undergoing COVID-19 treatment in hospital settings. The patch is a waterproof adhesive patch that sticks to the chest. It records ECG data which is transmitted via Bluetooth® to a smart phone app and from there is transmitted to a call center for analysis by a certified cardiac monitoring technician. Data from each patient is compiled at the center and findings are sent to providers and hospital facilities [13]. The below example (FIGURE 2) identifies the device; the specific privacy categories the device uses; and describes the third-party access by the monitoring center to the categories of the label.

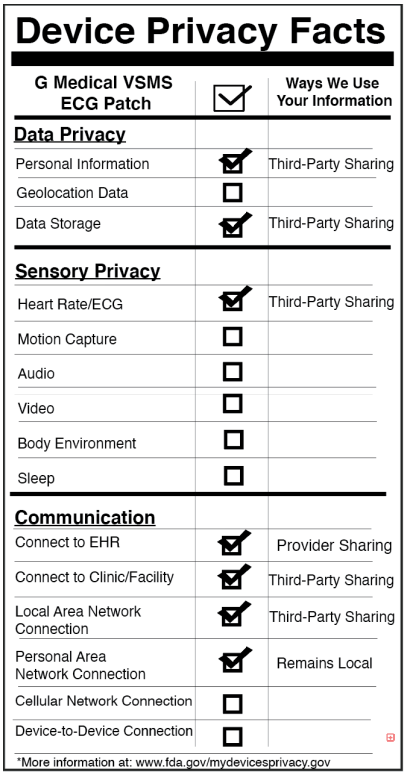

FIGURE 2: EXAMPLE LABEL FOR FDA APPROVED APP-ENABLED ECG PATCH [13]

In the ECG patch label example, it is demonstrated how device attributes and utilization are applied and communicated through this prototype label. Looking at the device literature filed with the FDA, we find that there is broad collection of personal information (both enrollment information and physiological data) by the patch device and that data is stored for review by analysis center before being given to providers (third-party sharing). The device example here is a hospital-based device so collection of geolocation information is not an attribute applicable in the example label but would apply to many other electronic medical devices. For sensory privacy information, the ECG patch is centrally focused on the collection of cardiological data which is transmitted to an off-site analysis center. This aspect is easily communicated by marking the "Heart Rate/ECG" category on the proposed label. In other devices, the wide array of sensory and physiological data collection types can be selected on the label to communicate other medically focused device attributes. For the communication label category, we look to the device function in connecting to Wireless Personal Area Networks via Bluetooth®; the ability to connect to the hospital local network; the third-party sharing of data to the analysis

center; and the return of that analysis to the EHR only between providers of analysis center and the hospital.

Overall, this is just one simple example of the label's application to a current electronic medical device. Ultimately, applicable authorities would need to further develop rules and guidelines to facilitate the common and uniform application of this label to devices. However, in this research it is important to not only discuss and develop a prototype privacy label, but to consider the mechanisms in which such a label could be implemented. Novel approaches in medical device design and policy need to be anchored by an understanding of their ability to be implemented which was both a consideration in the design and practical implication of this research.

3.3 Regulatory Framework and Implementation

A key service to the American people that the FDA is charged with is the assurance that the average consumer is dutifully represented in the standards created to protect and enable such consumers. In the last twenty years, the FDA and Congress have taken a special interest in labeling practices and the ways in which health risks, benefits, and information are communicated with the public. The Nutrition Labeling and Education Act of 1990 established mandatory nutrition labeling for packaged foods to enable consumers to make informed nutrition choices by adding Section 403(q) to the FFDCA [14]. This now synonymous labeling practice has been extremely successful in the education of consumers and studies have shown that individuals utilize the label and place a significant importance on label information. These nutrition labels are a shining example of the success of the labeling process and serve as a framework, consequently, for other labeling.

As electronic healthcare technology soldiers on, the FDA continues to maintain the regulatory tools and abilities to reflect their mission of consumer protection and health education in emerging areas. The implementation of privacy labeling for medical devices can follow the many examples of labeling programs that the FDA has facilitated in past years, including the nutritional label program and the current general device labeling requirements. The FDA could choose to amend Code of Federal Regulations 21 Section 801.4, the Labeling Requirements for Specific Devices, to require manufacturers to include a privacy label for electronic medical devices that collect/transfer patient data, wirelessly connect, have potential to impact patient safety, and/or other health related privacy concerns [14]. 21 CFR Section 801.4 already has been established by the FDA to define specialized labeling practices for unique categories of devices such as technical data pamphlets and package warnings for hearing aid products. Creating a classification for digital health products cleared and/or approved by the FDA within 21 CFR 801.4 would allow for privacy labeling measures to be implemented through the existing general device labeling code that manufacturers are familiar and already comply with.

This implementation process of a proposed rule and public comment for a privacy labeling regulation for electronic medical devices would be a significant opportunity to culminate existing research, gather expert opinions, and engage comments from stakeholders on label design, information, and attributes. This research study along with future work provides evidence and discussion, in addition to their traditional information sources, for regulatory agencies to make evidence-based decisions.

In short, the focus on modernizing labeling practices for the evolving world of medicine and products that fall under the authority of the FDA is not something new to the agency. In 2016, the FDA moved to revise 21 CFR 101.9 and 101.12, the nutrition label standards, because "there have been developments that have compelled us to reevaluate our regulations… to ensure that the Nutrition Facts label meets its intended goal of providing consumers information to assist them in maintaining healthy dietary practices. Specifically, such developments include the availability of newer consumption data, research…and the availability of recent consumer research on the use and understanding of the Nutrition Facts label" [14]. The FDA described the action in 2016 as essential in providing "consumers with more accurate and up-to-date information" regarding labels [14]. These aspects speak to not only the aforementioned authorities to change existing medical device labeling regulations, but that across the FDA's labeling profile the agency is taking steps to update and modernize.

Clearly, the agency speaks to these labeling regulations as an evolving process that should modernize for the best education of consumers in their decision making, whether it be selecting a food or understanding the privacy risk of their medical device.

3.4 Implications

The introduction of a privacy label has two aspects of impact: 1) an increase in consumer awareness and access to how their information is collected and used with medical devices; and 2) a mechanism in which the medical device industry will have to reflect on their data use and privacy standards as those practices are now in the light of public awareness. On the first point, the literature has described the impact that privacy awareness and education can have on individuals through their ability to make more informed decisions and reinforce their privacy values. This challenge is called the privacy paradox where people's intentions to maintain their privacy and avoid privacy-invasive behavior do not always match with their practiced behaviors, an issue of value compliance. Research on the privacy paradox has emphasized that "in order to enhance privacy… people should be reminded about their intentions to protect privacy during interactions. Therefore, tools and features need to be designed and developed that increase privacy awareness" [15]. The implication is that labeling can be that "reminder" tool and a centralized information location to make informed decisions that match an individual's privacy values.

Additionally, requiring greater consumer transparency with these devices will encourage manufacturers to evaluate their cybersecurity attributes and privacy policies. Labeling will require the industry members to think critically about their current privacy standards and observe their products through a lens of patient/provider safety, efficacy, and privacy intentions and values. With more specific health information categories displayed, there is greater likelihood that unnecessary privacy-

invasive measures (e.g. third-party sharing of data when only internal device personalization is necessary) will be eliminated to improve label appearances for concerned consumers.

Ultimately, the FDA has the regulatory framework for the labeling of devices with technical information, like privacy, and past successes in labeling. The FDA is a trusted name with consumers and industry sectors when it comes to consumer labeling which would support a successful implementation.

3.5 Limitations

The prototype privacy label proposed here, and the research study conducted does have some limitations. The major limitation is the validation of the privacy label tool in effectively communicating necessary information to consumers and other interested parties. Previously, extensive research has been conducted regarding the validation of a variety of food, privacy, and other types of consumer labels to ensure appropriate communication of determined attributes, readability of the label, and actual free-living use by consumers. This research study did not conduct a quantitative validation study of the proposed label, but it is timely to share this innovative healthcare focused privacy label design and assure that validation studies of the proposed label will be the topic of future research.

Additionally, a limitation of this privacy label research is the rapidly changing nature of electronic medical devices and new technology and capabilities. However, this prototype label has attempted to mitigate that limitation by reviewing the literature to find common, long-lasting attributes that can continually be communicated and by keeping selected categories as broad as possible while maintaining specificity for consumers. For example, the category of "Body Environment" is appropriately broad to encapsulate current device physiological measurements, like skin temperature, while being flexible for emerging device attributes such as sweat biomarker measuring. Ultimately, it would be important in implementation of this proposed label ensure that there are mechanisms to update such privacy label attributes as technology and consumer usage changes.

4. CONCLUSION

The increasing use of electronic medical devices are just one part of the connected world that is requiring devices to be designed and communicated for privacy and cybersecurity risks. Recent literature has focused on nutrition-like labels to communicate to consumers these risks, but these labels lack in specificity for the unique characteristics of electronic medical devices. Using the previous literature, we were able to develop a prototype privacy label specific to electronic medical devices needs that would integrate designed device cybersecurity and privacy features, communicate those designs and policies in a familiar format, and is feasible within existing regulation. As the healthcare field devolves electronically, so does the important mission of communicating medical device designs in terms of health data usage, cybersecurity, and consumer privacy.

ACKNOWLEDGEMENTS

Special thanks to Dr. Alexander H.K. Montoye and the GW CyberCorps program for inspiration, review, and support.

REFERENCES

[1] "What We Do: FDA Mission," last modified March 28, 2018, accessed February 22, 2021, https://www.fda.gov/about-fda/what-we-do.

[2] "PwC Consumer Intelligence Series: Protect Me," accessed February 22, 2021, https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html.

[3] "Privacy in Healthcare," accessed February 22, 2021, https://www.ama-assn.org/delivering-care/ethics/privacy-health-care.

[4] Pedersen, D. M., 1997, "Psychological Functions of Privacy," *Journal of Environmental Psychology* 17: 147-156.

[5] Aboujaoude, E., 2019, "Protecting privacy to protect mental health: The new ethical imperative," *Journal of Medical Ethics* 45(9): 604.

[6] "Towards Detecting Cocaine Use Using Smartwatches in the NIDA Clinical Trials Network (AutoSense)," last modified July 18, 2018, accessed February 22, 2021, https://clinicaltrials.gov/ct2/show/NCT02915341.

[7] Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A., 2020, "Healthcare Data Breaches: Insights and Implications," *Healthcare* 8(2): 133.

[8] Kelley, P. G., Cesca, L., Bresee, J., & Cranor, L. F., 2010, "Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach," *CMU CyLab* 9(14), 1-12.

[9] Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W, 2009, "A 'Nutrition Label' for Privacy," *SOUPS'09: Proceedings of the 5th Symposium on Usable Privacy and Security* 4(0), 1-12.

[10] "Apple App Privacy Details," accessed February 22, 2021, https://developer.apple.com/app-store/app-privacy-details/.

[11] "Privacy Label – Dutch Design Week," accessed February 22, 2021, https://ddw.nl/nl/programma/5024/privacy-label.

[12] Ates, H. C., Yetisen, A. K., Güder, F., Dincer, C., 2021, "Wearable devices for the detection of COVID-19," *Nature Electronics* 4, 13–14.

[13] "Remote or Wearable Patient Monitoring Devices EUAs," last modified June 25, 2020, accessed February 22, 2021, https://www.fda.gov/medical-devices/coronavirus-disease-2019-covid-19-emergency-use-authorizations-medical-devices/remote-or-wearable-patient-monitoring-devices-euas.

[14] "Labeling Requirements- Over-the-Counter (Non-Prescription) Medical Devices," last modified February 21, 2018, accessed February 22, 2021, https://www.fda.gov/medical-devices/general-device-labeling-requirements/labeling-requirements-over-counter-non-prescription-medical-devices.

[15] Potzsch, S., 2008, "Privacy Awareness: A Means to Solve the Privacy Paradox," *IFIP Advances in Information and Communication Technology* 298: 226-236.