



No exchange, same pain, no gain: Risk–reward of wearable healthcare disclosure of health personally identifiable information for enhanced pain treatment

Health Informatics Journal

2019, Vol. 25(4) 1675–1691

© The Author(s) 2018

Article reuse guidelines:

sagepub.com/journals-permissions

DOI: 10.1177/1460458218796634

journals.sagepub.com/home/jhi**Stephen Cory Robinson** 

Linköping University, Sweden

Abstract

Wearable technologies have created fascinating opportunities for patients to treat chronic pain in a discreet, mobile fashion. However, many of these health wearables require patients to disclose sensitive information, including health information (e.g., heart rate, glucose levels) and personal information (location, email, name, etc.). Individuals using wearables for treatment of chronic pain may sacrifice social health elements, including their privacy, in exchange for better physical and mental health. Utilizing communication privacy management, a popular disclosure theory, this article explores the policy and ethical ramifications of patients disclosing sensitive health information in exchange for better health treatment and relief of chronic pain. The article identifies scenarios where a user must disclose information, and what factors motivate or dissuade disclosure, and ultimately the use of a health wearable. Practical implications of this conceptual article include an improved understanding of how and why consumers may disclose personal data to health wearables, and potential impacts for public policy and ethics regarding how wearables and their manufacturers entice disclosure of private health information.

Keywords

disclosure, ehealth, health policy, health technology, pain management, privacy, wearables

Introduction

Populations across the world are aging¹ and headlines such as the “greying world” are becoming common in today’s media. With these demographic shifts, there come concerns regarding economic conditions, including overburdened healthcare systems.²

To better treat these aging populations and chronic health conditions, new technologies exist that can better treat conditions and patients through collection of sensitive data (glucose levels to

Corresponding author:

Stephen Cory Robinson, Department of Science and Technology, Linköping University, Campus Norrköping, 601 74 Norrköping, Sweden.

Email: cory.robinson@liu.se

monitor diabetes). However, concerns exist that current health privacy laws do not protect health information collected and serviced by smart technology and modern healthcare companies.^{3,4}

Adding to these concerns, consumers have identified health-related information as information they are least willing to disclose and perceive as one of the riskiest types of information to disclose.⁵ Recently, 55 percent of adults in the United States reported their “state of health” and current medications as very sensitive information.⁶ The sensitivity of personal health information is a legitimate concern. The sensitivity of health information is underscored as the U.S. government classifies health or medical information as *sensitive personally identifiable information (PII)*, or information “which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.”⁷ Due to the sensitivity of health information, it is recommended that stricter handling guidelines be enacted because of the increased risk to an individual if the data are exposed.⁷

Other concerns are apparent too, as wearable users report different levels and types of privacy concerns specific to the wearable they utilize.⁸ For example, with recent advances in technology, consumers and patients have new options for treating pain. The current state of healthcare technology provides individuals with mobile, discreet pain-treatment options. But with these conveniences in treatment come serious privacy and security concerns,⁹ including the sensitivity of the health information collected during usage of these pain-relieving devices, and how this information is collected, stored, and utilized.

This article explores current wearable technologies allowing individuals to treat chronic pain, and how the personal health information gathered by these devices is utilized. Using a theory of information disclosure, this article explores the disclosure scenarios faced by users of these devices. Exploring the risk–reward scenarios of disclosing sensitive health information in exchange for better pain treatment, this article questions whether these disclosure transactions are worthwhile. Implications for health information policy and data protection are examined as well.

Wearable healthcare

Defining wearable healthcare

Wearables, or a “computer or other electronic device that is small or light enough to be worn or carried on one’s body,”¹⁰ are now used for many health-related services. Many terms are utilized in today’s literature when describing new healthcare technology, including smart healthcare, digital health, ehealth, and mobile health. For clarity, this article only investigates healthcare wearables used in the treatment of chronic pain, and thus, this article refers to these devices as *wearables*.

Current wearable devices for pain

A plethora of wearables have been developed and marketed in recent years. Specifically, the number of pain relief devices for treatment of chronic pain have increased, and these pain relieving and pain-treatment devices deliver therapy through different technologies including infrared treatment (LumiWave device), transcutaneous electrical nerve stimulation (TENS), including iTENS, Enso, and the Quell wearable, and finally, Thync, a device that uses transcranial direct current stimulation (tDCS).

Each of these five health wearables collects different types of personal information. While every wearable does not require the use of a smartphone application or signing up for an online account, the devices are somewhat limited without the apps or online accounts. Together, the apps and user accounts allow a person to track usage, modify treatment, and be reminded of when to use the device or when supplies, such as electrodes, need replacing.

LumiWave, an Food and Drug Administration (FDA) approved device, is described by the company as an “automated, body-conforming LumiWave Infrared Light Therapy Device [...] offer[ing] you a safe and simple way to temporarily relieve minor pain and stiffness in your muscles and joints, without risking over treatment or causing unwanted side effects.”¹¹ LumiWave requires the disclosure of name, email address, physical address, telephone number, and “other details to help you with your experience.”¹² LumiWave does not have an accompanying smartphone application, nor does it appear that individuals need to create a user account via the company’s website.

“A modern day electrotherapy device that merges technology with the proven results of ‘TENS therapy’ to provide effective and lasting pain relief via a simple medical device app,”¹³ the iTENS device is one of two FDA-approved TENS devices currently available without a prescription to consumers. iTENS does not provide a privacy policy on their website but individuals are required to access it through the mobile application (iOS and Android platforms). Unlike other privacy policies that state what specific user information is collected, iTENS privacy policy is vague: “The application tracks usage data solely provided by the end user. The application stores this data on the device, and does not transmit any data or user information to iTENS or other third parties.”¹⁴ The iTENS device works through use of a smartphone application, and users are required to create a user account.

Formerly “Cūr,” and now referred to as “Enso,” another TENS therapy device, describes itself as “One button for pain relief.”¹⁵ When using services associated with the device, Enso collects a user’s name, email address, mailing address, mobile phone number, credit card number, date of birth, and location information.¹⁶ Enso has a corresponding smartphone application and requires users to sign up for a user account in order to utilize the application.

Another FDA-approved device, Quell is “100% drug free technology for managing chronic pain. Quell is designed for people with back pain, arthritis pain, nerve pain and leg and foot pain. Quell is doctor recommended.”¹⁷ The company’s privacy policy outlines types of personal information collected by the company: name, address, social media, Quell device information, location information, and analytics.¹⁸ Quell also has an accompanying smartphone application, but users are not required to create an account to utilize the application.

Described as a device that “uses neurosignaling to activate specific cranial and peripheral nerves to influence this balance and shift you to a state of calm or give you a boost of energy in minutes,”¹⁹ Thync can be used for pain relief, mindfulness, and other health activities. The Thync wearable is not approved by the FDA, but unlike the other devices in this article, it is exempt from FDA-clearance because it is considered a lifestyle product.²⁰ Thync requires the disclosure of name, email address, physical address, telephone number, and “other information that can be used to identify you” (Figure 1).²¹ The company may also obtain information from third parties and other sources outside of the company website and mobile app.²¹ Like several of the other devices, Thync utilizes a smartphone application and users must create an account to use the application. Importantly, the device does not work without the smartphone application; users control the device and start treatment only through the smartphone application.

How wearables improve the health/performance of people with chronic pain

An important feature of modern ehealth technologies is the potential to enhance the user’s quality of life, including the elderly, individuals with disabilities or those suffering from chronic pain.²² Dealing with the multiple aspects of pain management can become an overwhelming experience for individuals, and ultimately, efforts to control pain may actually decrease quality of life.²³ Through conveniences such as individualized, accessible pain management for chronic pain,

<

When is your birthday?

January	11	1993
February	12	1994
March	13	1995
April	14	1996
May	15	1997
June	16	1998
July	17	1999

What is your gender?

Male

Female

Sign Up

Figure 1. Thync application requesting user's date of birth and gender.

wearables may offer an opportunity to live a pain-free life, or experience less pain overall, and thereby increase quality of life.

Wearables available for treatment of chronic pain use a number of medical technologies for treating pain, and include ultrasound, TENS, and diathermy. One study examined the use of a wearable ultrasound device for patients experiencing chronic pain, and found a statistically significant reduction in pain and, relative to placebo, an improvement in health.²⁴ The underlying therapy for several of the discussed wearables is TENS, and the efficacy of TENS for treatment of chronic pain has been investigated thoroughly.^{25,26} Indeed, the literature suggests TENS is effective for treating chronic pain.^{27,28}

In addition to pain relief, it has been suggested that wearables have other benefits for quality of life and healthcare. They may not only potentially provide economic savings²⁹ but also increase the quality of care resulting from physician's time savings, remote patient monitoring, and more independent living for patients.²² Wearables, versus other health interventions (including delayed self-reporting via computer), can provide more individualized and instant patient feedback,³⁰ and monitor patients in a more comfortable, less expensive manner.⁹ The use of wearables can also decrease the dosage of narcotics necessary for managing pain; for example, two thirds of Quell users reported a reduction in use of pain medication while using the device.³¹ Ultimately, individuals may use wearables because the technology might improve access to health information, increase their ability to manage their health, or improve the quality of their healthcare.³²

Defining health

Health in the context of wearables is typically explored from the viewpoint of physical or mental health. However, the World Health Organization (WHO) defines health as “a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity.”³³ From this definition, it is vital to note that health is a triad of physical, mental, and social well-being.

As social health is important for overall health, wearables present some very important concerns for patients in that potential threats to social health may occur. Because wearables require disclosure of personal data, and the potential for privacy threats exist, patients are faced with the trade-off of whether decrease in chronic pain is worth the threats to social health. This trade-off, or risk–reward scenario, is an important phenomenon to explore when considering the use of wearables for the treatment of chronic pain.

Vulnerable state of sufferers of chronic pain

Individuals with chronic pain may have compromised decision-making capabilities^{34–40} as “chronic pain should be considered a ‘cognitive state,’ and that it may thus be competing with other cognitive abilities.”³⁴ Furthermore, daily coping of the multiple aspects of pain management can become an overpowering experience for individuals suffering from chronic pain.²³ Individuals with such compromised decision-making capabilities, according to Waisel’s definition,⁴¹ can be labeled a vulnerable population. “The vulnerable individuals’ freedom and capability to protect one-self from intended or inherent risks is variably abbreviated, from decreased freewill to inability to make informed choices.”⁴² Even with laws prohibiting use of genetic medical data for discriminative purposes,^{43,44} many negative scenarios face non-vulnerable individuals where sensitive health information can be misused, including abuse of health information in hiring decisions,^{45–48} and discrimination by insurers.⁴⁹ The importance of preventing misuse of vulnerable individuals’ information is of greater concern. It is crucial those suffering from chronic pain have their personal and health privacy protected. Furthermore, because sufferers of chronic pain may have compromised decision-making capabilities,^{34–40} manufacturers should clearly state the need for health information and why and how it is used. One way to better ensure privacy of sensitive personal and health information is through informed consent.

Informed consent refers to the conformity to the social rules of consent that require professionals to obtain consent from patients before proceeding with medical or therapeutic procedures.⁵⁰ Because health wearables offer both medical and therapeutic relief, the use of informed consent is paramount. Users of health wearables are able to give fully informed, valid consent if (1) they are competent to act, (2) receive a thorough disclosure (i.e. privacy policies, end user license agreement [EULA]), (3) comprehend the disclosure, (4) act voluntarily (not be forced by the manufacturer to disclose personal information), and finally, (5) consent to the intervention (i.e., by clicking “I Agree” when using the wearables associated smartphone application).⁵⁰

Theoretical framework

Risk–reward of disclosing

When individuals use wearables for treatment of chronic pain, they are required to disclose personal information to use the device and the associated smartphone application. For example, some wearables require patient’s gender, age, height, and weight (and other health information) to tailor the device’s treatment program, which in turn provides better treatment versus treatment not individualized for each patient. In this risk–reward scenario, disclosing information is a potential *risk*

Table 1. Sensitive stand alone and paired personal data/PII collected by wearables.

PII items collected by wearable	Name of wearable				
	LumiWave	iTENS	Enso	Quell	Thync
<i>Sensitive items if stand alone⁷</i>					
National identification number	—	—	—	—	—
Driver's license or state ID #	—	—	—	—	—
Passport number	—	—	—	—	—
Alien registration number	—	—	—	—	—
Financial account number	X	—	X	X	X
Biometric identifiers	—	—	—	—	—
<i>Sensitive items if paired with another⁷</i>					
Citizenship or immigration status	—	—	—	—	—
Medical information	X	X	X	X	X
Ethnic or religious affiliation	—	—	—	—	—
Sexual orientation	—	—	—	—	—
Last four digits of Social Security #	—	—	—	—	—
Date of birth	—	—	—	X	X
Criminal history	—	—	—	—	—
Mother's maiden name	—	—	—	—	—
<i>Other identifiers collected^{12,14,16,18,21}</i>					
Name	X	—	X	X	X
Physical address	X	—	X	X	X
Phone number	X	—	X	X	X
Email address	X	—	X	X	X
Location information	—	—	X	X	—
Social media account information	—	—	—	X	—
Analytics/Other information	X	X	X	X	X

PII: personally identifiable information.

to the user's privacy, while better targeted treatment or lessening of pain is a benefit, or *reward*. Importantly, the potential risk of losing privacy can be either theoretical⁵¹ or an observable, measurable risk.⁵

Because different types of personal information carry different levels of risk if disclosed or improperly exposed, it is important to differentiate between these different types of personal information (see Table 1). According to the United States Department of Homeland Security, specific types of information can be sensitive either by itself, or in combination with another identifier⁷. For example, an individual's national identification number is sensitive information alone, however, date of birth must be combined with another identifier to be considered sensitive.⁷

Using communication privacy management (CPM) theory, this article explores the disclosure and ethical scenarios faced by users of these devices. CPM has been utilized extensively for the purposes of exploring disclosure in technology and has extensive citation numbers: academic article searches for "CPM & technology" yielded 772 articles. The theoretical framework has been used in many realms of digital communication and technology, including social networks, blogs, and health communication, and is, therefore, applicable in exploring the disclosure aspect of health wearables for chronic pain treatment. Other research has explored conceptual privacy frameworks

by recommending frameworks and checklists for improving privacy wearables⁵² and how users have different levels and types of privacy concerns depending on the type of wearable utilized.⁸ However, as far as this author is aware, there are no current articles explicitly exploring CPM theory and disclosure of personal data in health wearables.

Several authors have attempted to conceptualize the idea of balancing or juggling the need to disclose information with perceived risks. The dilemma confronting users has been coined a privacy paradox.⁵³ By contrast, others have described it as a risk-benefit ratio.⁵⁴

Indeed, it seems that a paradox is present in online communication, specifically related to disclosure. If people sincerely perceive a level of risk when volunteering personal information to receive an online service, it is then argued that individuals would not involve themselves in this exchange. This notion of a privacy paradox⁵³ where individuals state their intention to limit disclosure, yet do the opposite by disclosing information, has been documented empirically.^{55–57} Scholars believe that the privacy paradox could be due to users' lack of awareness or literacy concerning privacy, however, the paradox has not fully been explained.⁵⁸

Health wearables: risk–reward of disclosing scenario

Whether lessening of chronic pain, or the possibility of better health treatment, both benefits are powerful motivators encouraging disclosure of sensitive health data that may sacrifice user privacy. A recent survey found that individuals are most willing to trade privacy for a benefit when related to medical and government information.⁵⁹ This author posits that pain relief may potentially be such a power motivator, a patient does not mentally process the risks associated with disclosure and continues ahead with disclosure even in the face of insecure infrastructure, untrusted entities, or insecure data transmission. In this scenario, the typical processing of risks and rewards might be absent because the reward is so enticing.

Given this risk–reward scenario (also referred to as *risk-benefit*) in disclosing personal data, why might sufferers of chronic pain risk disclosing their information (e.g., in light of unsecure infrastructure, unclear corporate rationale for collecting irrelevant health PII) in reward of better targeted, more effective treatment (lessening of pain, quicker relief of symptoms, etc.)? Ultimately, why are sacrifices of social health (invasion of privacy) worth the rewards of greater physical health (absence or lessening of chronic pain)? This conceptual paper explores these important questions.

Application of CPM

As posited in CPM theory, individuals make decisions about disclosure based on a rules-based system,⁵¹ ultimately attempting to minimize costs while maximizing rewards.⁶⁰ Risk-benefits ratio is one criteria individuals use in creating privacy rules or guidelines that dictate the ebb-and-flow of personal information.⁵⁴ CPM also states that privacy rules change such that as the perceived risk associated with information increases, the likelihood it will not be disclosed increases.⁶⁰

To conceptually explore disclosure between individuals and their wearables, it is important to identify the various parties and processes involved in disclosure transactions. For simplicity, two parties are involved in the disclosure transactions explored in this article: the individual using the wearable for treatment of chronic health conditions, or user, and the manufacturer of the wearable being used, or noted here as the company. CPM examines self-disclosure in relationships, and the user is seen as establishing a relationship with the company: the user must communicate with the company when setting up the device, or when experiencing product difficulties or technical issues. Importantly, one party is the disclosing party and the other is the recipient.⁵⁴ These roles are not static and can be

switched.⁵¹ For example, when the user submits an email to the company, the user is the disclosing party and the company is the recipient. However, when the company sends a reply email to the user, the company then becomes the disclosing party and the user becomes the recipient.

Both parties involved in the disclosure are constantly balancing disclosure and concealing private information.⁵¹ Furthermore, both parties follow basic rules that determine this constant balancing of disclosure or keeping information private. At its foundation, CPM is guided by three assumption maxims that define the managing of private disclosure, while the interaction maxims elucidate how interactions with others are managed.⁵¹

The following section explores the three assumption maxims and three interaction maxims, specifically illustrating how each is present in the risk–reward scenario faced by users disclosing personal data to the company when using a health wearable.

Public–private dialectical tension

When an individual contemplates disclosing information, there are forces pulling toward both the need for privacy through hiding information and being public through divulging. For the discloser, the pressure between remaining private and publicly revealing information is a difficult situation. The extent to which the information becomes public information depends on to whom the information is disclosed, and how many people it is disclosed to, among other factors.

The public–private tension of disclosure is apparent when a sufferer of chronic pain decides to use a wearable for pain treatment. Using a wearable as such requires the user to cognitively process the pull of remaining private through concealing information while also balancing the pull of disclosing the information necessary to use the wearable and smartphone application. Once information is disclosed, a wearable user should expect decreased privacy levels of their information: it is not always clear who they are disclosing information to, and how many individuals or companies have access to the information.

Individuals using wearables may, for the first time in life, contemplate the public–private dialectical tension of disclosing their personal information. The risks associated with disclosing information to a wearable may not have been apparent in previous experiences, including during a visit to a doctor. If these individuals have sought healthcare treatment before, it should be assumed they are familiar disclosing information necessary for receiving treatment from a physician. When visiting a physician, the patient might be asked to provide their date of birth, telephone number, credit card (for payment purposes), and health history. Because 13 percent of physicians in the United States still utilize paper-based medical records,⁶¹ and electronic health records (EHRs) are a top factor for physician dissatisfaction,⁶² the patient may assume the information is stored locally in the office in the form of a paper record, and therefore protected from unauthorized access. Furthermore, the individual may assume the physician is a trustworthy source, as a physician is a publicly respected position. Finally, the individual must disclose information, including health history, for proper health treatment to be received. These experiences are vastly different than those experienced when using a wearable for pain treatment for the first time. The levels of disclosure and experience of trust associated with visiting a physician may setup unrealistic trust and disclosure expectations when using a wearable.

Conceptualization of private information

Private information, according to CPM, can be conceptualized in the sense of who owns the information. Along with owning personal information, any individual has the right to control access to it, and consequently, decides whether to disclose the information or keep it private.⁵⁴

Whether an individual directly purchases a wearable for themselves, received it from a physician, or as a gift from a family member or friend, every wearable user must decide initially if they believe using a specific wearable is worthwhile. Users of some wearables are required to utilize the corresponding smartphone application or signup for a user account through the company's website. Specifically, most of the devices with accompanying smartphone applications previously overviewed in this article require users to sign up for an account to operate the application. Also, devices like Thync require users to download the application to use the device. While a user may decide ultimately to not use the wearable because they do not want to disclosure information, it can be argued they have already decided to keep the wearable because of their completed purchase intention. Faced with treating their chronic pain or not using the wearable due to disclose of their personal information, it seems most would decide to keep the wearable rather than sacrifice potential treatment. Again, the user faces the risk–reward scenario.

It is important to note that a second risk–reward scenario is highlighted here: As noted, the user not only faces the risk–reward scenario of treatment of chronic pain versus disclosure of personal information, but they face a second scenario as well: deciding whether to purchase the wearable or not because of unknown requirements for disclosure. For example, companies may lack privacy policies or make it difficult to access (iTENS' users can only locate the company's privacy policy in the application, but not on the company's website).¹⁴ Users must proactively decide whether purchasing a wearable is worthwhile in the face of unknown or vague disclosure practices. By placing this extra burden on users, companies are complicating the process of receiving healthcare. Because users already face a multitude of issues while balancing life and their chronic pain,²³ companies should streamline access to healthcare by clearly informing disclosure practices prior to purchases. Only then can users be informed what disclosure decisions are required and ultimately if the wearable is worthwhile.

Privacy rules

Several criteria affect how individuals make rules for whether to disclose or not. This is not the actual decision of whether to disclose or not, but how users come to that decision. Criteria influencing these guidelines include gender, culture, motivation, and other factors.⁵⁴

Included in these criteria might be one's current state of health. Because chronic pain may influence decision-making,^{34–40} the author argues that overall health is an important criterion to consider in addition to CPM's criterion of motivation, gender, and culture. Users must account for their own pain levels and state of social, mental, and physiological health when making decisions. Furthermore, companies should understand that individuals suffering from chronic pain may be impaired when making decisions, and companies should not make emotional appeals to sway healthcare-related purchasing decisions.

Shared boundaries

With shared boundaries, the recipient of the information becomes co-owner, and both parties cooperate to create a “mutual boundary around the information”, with different boundaries existing for sharing information with groups, families, or dyads.⁵⁴

Conflicting with CPM's co-ownership of information, users of wearables do not own their data, instead the data are owned by the company manufacturing the device.⁹ Further surprising, some companies charge consumers a monthly fee to access raw health metrics. This apparent conflict in disclosing private information to wearables means that users are not always consciously aware how the company discloses the information to third parties. While users may be notified of these

sharing practices in the company's user agreement or privacy policy, research shows that many users are not aware of them or do not read such policies,⁶³ and in turn, are not aware to the extent their information is shared.

Shared boundaries, in terms of disclosing health information to the company, potentially sets up the user for some risky situations. Because some wearables are easy to hack due to their inherent communication technologies,⁶⁴ as observed in glucose pumps and wireless digital pacemakers,^{65,66} users could face significant privacy risks, including their patient data being compromised, distorted, or lost.⁹ Hacking is, indeed, a significant threat facing users of wearables.^{67–69} Because medical information is sensitive, and medical identity theft is increasing exponentially,⁷⁰ it is critical that users be aware of the risks involved with using a wearable, and that companies employ reliable security to protect users' personal data.

Boundary coordination

Referring to how individuals co-own and co-manage their personal information, boundary coordination involves three processes: regulating boundary linkages, boundary ownership rights, and boundary permeability.⁵⁴ These processes involved in boundary coordination are explained⁶⁰:

As part of the coordination process, individuals enact rules to moderate boundary linkages (whether to link to others), boundary ownership rights (who should be included or excluded in the boundary), and boundary permeability (what information may be revealed to whom).⁶⁰ (p. 336)

At the onset of using a wearable, individuals are faced with the decision of whether to include the wearable manufacturer and create a boundary linkage. In essence once the user moves past the EULA, the user has agreed to create a boundary linkage with the wearable company. For example, if a user purchases a Quell device, downloads the app on their smartphone, agrees to the EULA, and pairs the wearable with their smartphone, they have initiated and created a boundary linkage with the device's manufacturer.

Boundary linkages may also occur with which entities the user is not even aware. When users download an application to their smartphone, they may unknowingly give permission for their location and other sensitive information to be tracked and shared for advertising purposes.⁷¹ In this instance, users are not consciously creating boundary linkages, and, therefore, not able to setup ownership rights and the corresponding boundary permeability.

The same scenario applies when users create the boundary linkage with the manufacturer of the health wearable. The manufacturer may share personal information with other companies in efforts to better profile the consumer or offer additional products or services. The user is not included in the decision-making process of who should be included or excluded in the boundary, and what information is revealed to whom. Furthermore, the information collected and shared by mobile applications may be shared over insecure network connections, and as one study found, may be sent to North America, regardless of where the user is located.⁷² Clearly, wearable users may have little or no decision with regards to creating boundary linkages, ownership rights, or the boundary permeability.

Boundary turbulence

Boundary turbulence occurs when there are violations of rules created by the parties involved with the disclosure of information.⁵⁴ When boundary turbulence happens, different levels of breakdown may play out, and users may experience collapse or disruption while managing their information.⁷³

Regarding our wearables user, privacy violations can occur when the company attempts to access information the user deems unnecessary to the disclosure transaction. An example is when the company attempts to access things seemingly unrelated to the treatment of pain in attempts to collect personal information for marketing purposes and selling of information to third parties. As highlighted earlier, companies may attempt to access the user's smartphone applications, access to camera and the user's photos or videos, access to their contacts, and/or use of GPS location tracking. Also, some companies ask users for their social network accounts.¹⁸

When these violations occur, the user may feel violated by the company, and their mental health may suffer. If companies access users' social account information, they may potentially violate not just the users, but the user's family and friends. These far reaching violations could deeply affect the user's social health, as the friends and family who are violated may react in many negative ways (e.g., deleting online friendship, not returning communication).

Individuals living with chronic pain already experience scenarios where their medical condition impacts their relationships with friends and family, including themes of family loss (e.g., financial losses, loss of family or friendships, or loss of social activities), life changes (in relationships, or career/employment prospects), emotional impact of pain (including self-blame for changes caused for family, and emotions of anger and fear), and future plans (expected outcomes of illness, or ability to survive the experience).⁷⁴ The disclosure of one's chronic illness or medical condition via social media can further complicate relationships—broader social forces already put individuals with chronic pain at a disadvantage.⁷⁵ Individuals with chronic pain may receive negative social judgments as they are perceived as having less emotional warmth and being less competent versus individuals without chronic pain,⁷⁶ among many negative stigmas related to chronic illness.⁷⁵ Individuals with chronic pain may be labeled members of the "out group," and in the context of pain, observers, which can include friends and family, have less altruistic motivation and feel less empathy toward members of social out-groups.^{77,78} The chronic pain of the individual in their family can be determinants of family dynamics and degree of family satisfaction.⁷⁹ Rapid estimations of trustworthiness, with no basis in fact, can affect judgments of authenticity of individuals in pain,⁷⁵ and because individuals with chronic pain are more vulnerable to frequent social conflicts⁸⁰ and higher reactivity to interpersonal stressors,⁸¹ friends or family of individuals with chronic pain may lessen social interactions. By extension, the disclosure of an individual's chronic illness or medical condition can have significant, negative social consequences both in physical and digital environments, including social media.

In addition, given that sensitive health information can be misused in hiring decisions^{45–48} and discrimination by insurers,⁴⁹ even while such discriminatory acts are illegal,^{43,44} individuals with chronic pain may not want their health information disclosed for fear of how employers or insurers may view or use the information.

The application of a disclosure theory in the use of wearables for treatment of chronic pain has revealed important disclosure scenarios and consequences stemming from manufacturers collection of users' personal information. Concluding the application of the theory's tenets, it is clear that individuals using wearables face complicated disclosure scenarios that may result in severe risks including loss of privacy, potential identity theft, altering or loss of health records, and hacking. Simply put, the use of wearables for treatment of chronic pain brings with it a risky balance and potential loss of social, psychological, and mental health.

Implications

A common thread found in the privacy policies of five current pain-relief health wearables is the collection of sensitive personal information. While individuals may need to provide name and

email to register an account and pair it with the health wearable, it is concerning that companies are also accessing location information, social media accounts, and so on. In today's risky start-up scene, many companies feel financial pressure to collect and sell personal information. Because these companies stress the pain-relieving abilities of their devices, potential users may be even more inclined to purchase and agree to insecure data collection policies. Companies involved in healthcare, specifically those mentioned in this article, have legal and practical responsibilities to protect their customers' sensitive personal information. The author sees a real need for establishing frameworks dictating what types of data can be collected by wearable healthcare devices and how the data collected can be utilized by device manufacturers. Without the proper frameworks in place, companies can continue to disregard consumer and patient privacy and misuse sensitive information with the guise of pain relief and better quality of life.

The author recommends that wearable manufacturers be required to provide clear, concise information about their information collection practices, and only require disclosure of information directly related to delivering appropriate treatment (gender and age to better target treatment levels), or identifying the level of treatment necessary (i.e. pain levels). Individuals with chronic pain already face a multitude of issues while balancing life and their chronic pain,²³ and these should not include extra burdens of navigating the complicated disclosure scenarios and privacy risks associated with using a wearable for pain relief. Those suffering from chronic pain may have impaired decision-making capabilities,³⁴⁻⁴⁰ and, therefore, it is even more important that sound policies are in place to protect the sensitive health information of these vulnerable populations.

Wearable manufacturers should clearly state what information is being collected, who it is being shared with, and how users can opt-out, if so desired. More specifically, industry should allow individuals to apply detailed controls of how data are shared, what is collected, and when and who has access to the data.⁸ Companies should streamline access to healthcare by clearly informing users of their information collection and sharing practices. Privacy policies and EULAs describing information collection practices are often dense and confusing, and research shows that many users are not aware of them, because they do not read such policies⁶³ or ignore notifications.⁸²

In addition to clear policies noting who owns the data collected and data utilized by wearables, particular attention should be paid to data ownership when a manufacturer goes bankrupt or ceases operations. In examples where companies have gone bankrupt, the value of personal data owned by corporations has had important impacts on consumers. Two recent rulings in the United States highlight the importance of this issue. First, Sports Authority, a US-based sporting goods store, finalized its bankruptcy proceedings by ultimately selling its assets, including collected consumer data, to its competitor. For the competitor, Dick's Sporting Goods, the value of the consumer data was clear: a rare opportunity for collecting valuable consumer insights, including the ability to analyze regions where customers were especially loyal to Sports Authority, why consumers preferred Sports Authority versus Dick's Sporting Goods, and most importantly, to solicit customers' business.⁸³ Second, in the case of RadioShack, an American electronics retailer, the company argued that its privacy policy statement not to sell consumer information should not be enforced. Intervention from the US Federal Trade Commission (FTC) advised RadioShack to sell consumer information as a package with its retail stores.⁸⁴ The issue of data ownership is particularly relevant for wearable users, as the manufacturer of iTENS, one wearable discussed in this article, refers to data ownership in their privacy policy¹⁴:

If iTENS is involved in a merger, acquisition, or sale of all or a portion of its assets, you will be notified via email and/or a prominent notice on our web site of any change in ownership or uses of this information, as well as any choices you may have regarding this information.

This article has documented the many advantages of wearables, including their ability to increase individuals' physical and psychological health through reduction of pain. However, wearables can also violate elements of social health, by requesting access to unnecessary personal information, including details about users' social media accounts. If a user's information has been compromised, it is possible that unauthorized access to their social media accounts may occur. If their social media accounts are compromised, it could lead to possible violations for family and friends. By potentially creating conflict in relationships, wearables can have the undesired and opposite effect on health by negatively affecting one's social health.

Regarding the marketing of wearables, the author sees important practices for clearer marketing and advertising practices. Wearables are modern technological devices that employ proven marketing practices, including cotemporary advertising campaigns and fancy packaging design. Individuals with chronic pain may have compromised decision-making capabilities,³⁴⁻⁴⁰ and, therefore, manufacturers should not make emotional advertising appeals. By doing so, companies are potentially abusing customers who are simply seeking relief of pain and better quality of life. When marketing products, it is recommended that manufacturers of health wearables present simple, true statements regarding the benefits of the technology.

Finally, the author notes an important aspect of wearables that may impact one's ability to acquire them: financial cost. Many of the wearables mentioned in this article require users to have a smartphone to operate the wearable or enhance the user's experience. Individuals suffering from chronic pain come from diverse socioeconomic backgrounds. Unfortunately, because many wearables require an accompanying mobile application, users may be required to purchase a smartphone, potentially putting treatment that much farther out of reach financially. It should not be assumed every potential user already owns a smartphone: only 77 percent of Americans own a smartphone,⁸⁵ reports note the first decline in smartphone adoption in 14 years,⁸⁶ and trends toward less complicated "feature phones" are gaining in popularity, too.^{87,88} Moreover, costs of wearables are typically not paid for by insurance, so consumers often pay the full retail price. Also, because many wearables initially begin as crowdfunded projects (including four wearables discussed earlier in the article: Quell, Enso, LumiWave, and iTENS) and not all crowdfunded technologies come to fruition, some individuals may suffer financial losses. Individuals also have to replace electrodes after a certain amount of time, leading to a long-term financial commitment. By allowing wearables to operate without the need for pairing with a smartphone application, risks of data collection concerns are lessened and rewards of purchasing the wearable are increased.

Future studies

This conceptual paper has provided a potential framework for future empirical studies. It would be worthwhile to carry out empirical work to investigate actual perceptions of disclosing personal data to health wearables in exchange for pain relief or better health treatment. This conceptual article raises many questions suitable for empirical study: If users are provided with data collection practices prior to purchasing a specific wearable, are they more willing to purchase the device and allow for the data collection required for treatment? Furthermore, are individuals willing to disclose highly sensitive personal data in exchange for better targeted health treatments and potentially lessening of chronic pain? Are chronic pain sufferers who use wearables for pain treatment more willing to utilize a wearable in combination with a smartphone app when "enhanced" treatment options are only available via the application? In addition, are sufferers of chronic pain, due to their compromised decision-making capabilities, able to give fully informed consent to collect their personal information? Are sufferers of chronic pain able to comprehend the full complexities related to disclosure of their personal information while using health wearables for treatment of chronic pain?

Conclusion

Ultimately, consumers and individuals with chronic pain are faced with the dilemma: “Is sacrificing social health, including privacy, worth the mental and physical benefits brought by the use of health wearables?” The relief of chronic pain can be a powerful motivator for individuals to disclose their sensitive health information. Disclosing personal information for pain relief is a modern day risk–reward scenario that many individuals will face as the adoption of health wearables increase. In a perfect world, individuals would be able to maintain physical, psychological, and social health, without having to sacrifice or lessen one of the other three areas. Patients currently experiencing pain, however, are constantly juggling this risk–reward conflict when they use health wearables. Lessening of pain increases quality of life, but disclosing personal data when using health wearables sacrifices their social health. In order to achieve complete health—a combination of physical, mental, and social health—consumer technology companies and chronic pain sufferers alike must be willing to seek an agreeable scenario where disclosing personal data provides better targeted health outcomes while the privacy and protection of personal health information are upheld.


Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Stephen Cory Robinson  <https://orcid.org/0000-0003-1253-9671>

References

1. Kalache A and Keller I. The greying world: a challenge for the twenty-first century. *Sci Prog* 2000; 83(Pt. 1): 33–54.
2. Bloom DE, Chatterji S, Kowal P, et al. Macroeconomic implications of population ageing and selected policy responses. *Lancet* 2015; 385: 649–657.
3. Koontz L. Health information privacy in a changing landscape. *Generations* 2015; 39: 97–104.
4. Langley MR. Hide your health: addressing the new privacy problem of consumer wearables. *Georgetown Law J* 2015; 103: 1641–1659.
5. Robinson C. Disclosure of personal data in ecommerce: a cross-national comparison of Estonia and the United States. *Telemat Inform* 2017; 34: 569–582.
6. Rainie L. *The state of privacy in America: what we learned*. Washington, DC: Pew Research, 2016.
7. Callahan ME. *Handbook for safeguarding sensitive personally identifiable information*. Washington, DC: United States Department of Homeland Security, 2012.
8. Motti VG and Caine K. Users’ privacy concerns about wearables: impact of form factor, sensors and type of data collected. In: Brenner M, Christin N, Johnson B, et al. (eds) *International Conference on Financial Cryptography and Data Security*. Berlin; Heidelberg: Springer Berlin Heidelberg, 2015, pp. 231–244.
9. Piwek L, Ellis DA, Andrews S, et al. The rise of consumer health wearables: promises and barriers. *PLoS Med* 2016; 13: 1–9.
10. Oxford Dictionary. Definition of wearable in English, 2014, <https://en.oxforddictionaries.com/definition/wearable> (accessed 27 August 2018).
11. BioCare Systems. LumiWave—infrared light therapy pain relief, 2016, <http://www.lumiwave.com>

12. LumiWave. Privacy policy, <https://www.lumiwave.com/privacy-policy> (accessed 19 March 2018)
13. iTENS. iTENS, 2016, <http://itens.com/index.html>
14. iTENS. Privacy statement, 2017, <https://itunes.apple.com/us/app/itens/id1058254325?mt=8>
15. CUR. CUR—professional pain therapy evolved into a patch, 2016, <http://cur.me>
16. Thimble Bioelectronics. Privacy policy (United States), 2017, <https://ensorelief.com/privacy/>
17. Neurometrix. Chronic pain relief—drug free and doctor recommended, 2016, <https://www.quellrelief.com/chronic-pain>
18. Neurometrix. Privacy policy for Quell, 2018, <https://www.quellrelief.com/privacy>
19. Thync. Science/technology, 2015, <http://www.thync.com/science-and-technology>
20. Thync. FAQ: how has Thync been working with the FDA? 2015, <http://support.thync.com/articles/FAQ/H08>
21. Thync. Privacy policy, 2017, <http://www.thync.com/privacy-policy>
22. Park S and Jayaraman S. Smart textile-based wearable biomedical systems: a transition plan for research to reality. *IEEE T Inf Technol B* 2010; 14: 86–92.
23. McCracken LM, Carson JW, Eccleston C, et al. Acceptance and change in the context of chronic pain. *Pain* 2004; 109: 4–7.
24. Lewis GK Jr, Langer MD, Henderson CR Jr, et al. Design and evaluation of a wearable self-applied therapeutic ultrasound device for chronic myofascial pain. *Ultrasound Med Biol* 2013; 39: 1429–1439.
25. Johnson MI and Bjordal JM. Transcutaneous electrical nerve stimulation for the management of painful conditions: focus on neuropathic pain. *Expert Rev Neurother* 2011; 11: 735–753.
26. Pivec R, Stokes M, Chitnis AS, et al. Clinical and economic impact of TENS in patients with chronic low back pain: analysis of a nationwide database. *Orthopedics* 2013; 36: 922–928.
27. Jin DM, Xu Y, Geng DF, et al. Effect of transcutaneous electrical nerve stimulation on symptomatic diabetic peripheral neuropathy: a meta-analysis of randomized controlled trials. *Diabetes Res Clin Pr* 2010; 89: 10–15.
28. Sluka KA, Bjordal JM, Marchand S, et al. What Makes transcutaneous electrical nerve stimulation work? Making sense of the mixed results in the clinical literature. *Phys Ther* 2013; 93: 1397–1402.
29. Robinson S, Stroetmann KA and Stroetmann VN. Tele-homecare for chronically ill persons: pilot trials, medical outcomes and future perspectives. *Stud Health Technol* 2004; 103: 197–205.
30. Swan M. Emerging patient-driven health care models: an examination of health social networks, consumer personalized medicine and quantified self-tracking. *Int J Env Res Pub Health* 2009; 6: 492–525.
31. Anderson P. Wearable nerve stimulator improves chronic pain, 2015, <http://www.medscape.com/view-article/851131>
32. Li H, Wu J, Gao Y, et al. Examining individuals' adoption of healthcare wearable devices: an empirical study from privacy calculus perspective. *Int J Med Inform* 2016; 88: 8–17.
33. World Health Organization. *Preamble to the constitution of the world health organization as adopted by the international health conference*, New York, 19–22 June, 1946; signed on 22 July 1946 by the representatives of 61 States (Official Records of the World Health Organization, no. 2, p. 100) and entered into force on 7 April 1948, <http://www.who.int/about/mission/en/> (accessed 27 August 2018).
34. Apkarian AV, Sosa Y, Krauss BR, et al. Chronic pain patients are impaired on an emotional decision-making task. *Pain* 2004; 108: 129–136.
35. Baliki MN, Geha PY, Apkarian AV, et al. Beyond feeling: chronic pain hurts the brain, disrupting the default-mode network dynamics. *J Neurosci* 2008; 28: 1398.
36. Eccleston C and Crombez G. Pain demands attention: a cognitive–affective model of the interruptive function of pain. *Psychol Bull* 1999; 125: 356–366.
37. Hess LE, Haimovici A, Muñoz MA, et al. Beyond pain: modeling decision-making deficits in chronic pain. *Front Behav Neurosci* 2014; 8: 263.
38. Montoya P, Sitges C, García -Herrera M, et al. Abnormal affective modulation of somatosensory brain processing among patients with fibromyalgia. *Psychosom Med* 2005; 67: 957–963.
39. Verdejo-García A, López-Torrecillas F, Calandre EP, et al. Executive function and decision-making in women with fibromyalgia. *Arch Clin Neuropsychol* 2009; 24: 113–122.
40. Walteros C, Sánchez -Navarro JP, Muñoz MA, et al. Altered associative learning and emotional decision making in fibromyalgia. *J Psychosom Res* 2011; 70: 294–301.

41. Waisel DB. Vulnerable populations in healthcare. *Curr Opin Anaesthesiol* 2013; 26: 186–192.
42. Shivayogi P. Vulnerable population and methods for their safeguard. *Perspect Clin Res* 2013; 4: 53–57.
43. Council of Europe, *Recommendation Cm/rec(2016) 8 on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests*. Strasbourg: Council of Europe, 2016.
44. Joly Y, Feze IN, Song L, et al. Comparative approaches to genetic discrimination: chasing shadows? *Trends Genet* 2017; 33: 299–302.
45. Greenhouse S and Barbaro M. Wal-Mart memo suggests ways to cut employee benefit Costs, 2005, <http://www.nytimes.com/2005/10/26/business/walmart-memo-suggests-ways-to-cut-employee-benefit-costs.html> (accessed 24 August 2016).
46. Hoffman S. Employing e-health: the impact of electronic health records on the workplace. *Kansas J Law Public Policy* 2009; 19: 409.
47. Ajunwa I. Workplace Wellness programs could be putting your health data at risk, 2017, <https://hbr.org/2017/01/workplace-wellness-programs-could-be-putting-your-health-data-at-risk>
48. Zarya V. Employers are quietly using big data to track employee pregnancies, 2016, <http://fortune.com/2016/02/17/castlight-pregnancy-data/>
49. Pritts J. The importance and value of protecting the privacy of health information, 2008, <http://www.iom.edu/CMS/3740/43729/53160.aspx>
50. Beauchamp TL and Childress JF. *Principles of biomedical ethics*. 7th ed. New York: Oxford University Press, 2013.
51. Petronio S. *Boundaries of privacy dialectics of disclosure*. Albany, NY: State University of New York Press, 2002.
52. Safavi S and Shukur Z. Conceptual privacy framework for health information on wearable device. *PLoS ONE* 2014; 9: e114306.
53. Barnes SB. A privacy paradox: social networking in the United States. *First Monday* 2006; 11, <http://firstmonday.org/article/view/1394/1312>
54. Petronio S and Durham W. Communication privacy management theory. In: Baxter L and Braithewaite D (eds) *Engaging theories in interpersonal communication: multiple perspectives*. Thousand Oaks, CA: SAGE, 2008, pp. 309–322.
55. Norberg PA, Horne DR and Horne DA. The privacy paradox: personal information disclosure intentions versus behaviors. *J Consum Aff* 2007; 41: 100–126, <http://onlinelibrary.wiley.com/journal/10.1111/%28ISSN%291745-6606/issues>
56. Yao MZ, Rice RE and Wallis K. Predicting user concerns about online privacy. *J Am Soc Inf Sci Tec* 2007; 58: 710–722.
57. Youn S and Hall K. Gender and online privacy among teens: risk perception, privacy concerns, and protection behaviors. *Cyberpsychol Behav* 2008; 11: 763–765.
58. Taddicken M. The “privacy paradox” in the social web: the impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *J Comput-Mediat Comm* 2014; 19: 248–273.
59. EMC. EMC privacy index, 2014, <http://www.emc.com/campaign/privacy-index/index.htm?pid=home-emcprivacyindex-120614>
60. Metzger MJ. Communication privacy management in electronic commerce. *J Comput-Mediat Comm* 2007; 12: 1–27.
61. Office of the National Coordinator for Health Information Technology. Office-based physician electronic health record adoption, Health IT Quick-Stat #50, 2016, <https://dashboard.healthit.gov/quickstats/pages/physician-ehr-adoption-trends.php>
62. Friedberg MW, Chen PG, Van Busum KR, et al. *Factors affecting physician professional satisfaction and their implications for patient care, health systems, and health policy*. Santa Monica, CA: RAND Corporation, 2013.
63. Smith A. Half of online Americans don’t know what a privacy policy is, 2014, <http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is>
64. Kirk S. The wearables revolution: is standardization a help or a hindrance? Mainstream technology or just a passing phase? *IEEE Consumer Elec Mag* 2014; 3: 45–50.

65. Halperin D, Heydt -Benjamin TS, Fu K, et al. Security and privacy for implantable medical devices. *IEEE Pervas Comput* 2008; 7: 30–39.
66. Maisel WH and Kohno T. Improving the security and privacy of implantable medical devices. *New England Journal of Medicine* 2010; 362: 1164–1166.
67. Hilts A, Parsons C and Knockel J. Every step you fake: a comparative analysis of fitness tracker privacy and security. *Open Effect Report*, 2016, https://openeffect.ca/reports/Every_Step_You_Fake.pdf
68. Karkazis K, Fishman JR. and Tracking U.S. professional athletes: the ethics of biometric technologies. *Am J Bioeth* 2017; 17: 45–60.
69. Troiano A. Wearables and personal health data: putting a premium on your privacy. *Brooklyn Law Review* 2017; 82: 1715–1753.
70. Krishnan R, Rainwater R and FitzGerald D. Risk based medical identity theft prevention. Google Patents 2018, <https://patentimages.storage.googleapis.com/91/73/23/1b9128b3daace5/US20180018747A1.pdf> (2018, accessed 27 August 2018).
71. Almuhammedi H, Schaub F, Sadeh N, et al. Your location has been shared 5,398 times! A field study on mobile app privacy nudging. In: Proceedings of the 33rd annual ACM conference on human factors in computing systems, Seoul, Republic of Korea, 18–23 April 2015, pp. 787–796. New York, ACM.
72. Ferreira D, Kostakos V, Beresford AR, et al. Securacy: an empirical investigation of Android applications' network usage, privacy and security. In: Proceedings of the 8th ACM conference on security & privacy in wireless and mobile networks, New York, 22–26 June 2015, pp. 1–11. New York: ACM.
73. Child JT and Westermann DA. Let's be Facebook friends: exploring parental Facebook friend requests from a communication privacy management (CPM) perspective. *J Fam Commun* 2013; 13: 46–59.
74. West C, Usher K, Foster K, et al. Chronic pain and the family: the experience of the partners of people living with chronic pain. *J Clin Nurs* 2012; 21: 3352–3360.
75. Williams AC. Defeating the stigma of chronic pain. *Pain* 2016; 157: 1581–1582.
76. Ashton-James CE, Richardson DC, de CWAC, et al. Impact of pain behaviors on evaluations of warmth and competence. *Pain* 2014; 155: 2656–2661.
77. Gutsell JN and Inzlicht M. Empathy constrained: prejudice predicts reduced mental simulation of actions during observation of outgroups. *J Exp Soc Psychol* 2010; 46: 841–845.
78. Mathur VA, Harada T, Lipke T, et al. Neural basis of extraordinary empathy and altruistic motivation. *Neuroimage* 2010; 51: 1468–1475.
79. Collado A, Gomez E, Coscolla R, et al. Work, family and social environment in patients with Fibromyalgia in Spain: an epidemiological study: EPIFFAC study. *BMC Health Serv Res* 2014; 14: 513.
80. Feldman SI, Downey G and Schaffer-Neitz R. Pain, negative mood, and perceived support in chronic pain patients: a daily diary study of people with reflex sympathetic dystrophy syndrome. *J Consult Clin Psych* 1999; 67: 776–785.
81. Zautra AJ, Hamilton NA and Burke HM. Comparison of stress responses in women with two types of chronic pain: fibromyalgia and osteoarthritis. *Cognitive Ther Res* 1999; 23: 209–230.
82. Anthes G. Data brokers are watching you. *Commun ACM* 2015; 58: 28–30.
83. Schiffer A. In Sports Authority bankruptcy, customer e-mail data commands hefty sum. *Los Angeles Times*, 2016, <http://www.latimes.com/business/la-fi-sports-authority-auction-20160629-snap-story.html>
84. Mayfield J. FTC requests bankruptcy court take steps to protect radioshack consumers' personal information. *Letter to Consumer Privacy Ombudsman Describes Possible Conditions on Sale of Data*, 2015, <https://www.ftc.gov/news-events/press-releases/2015/05/ftc-requests-bankruptcy-court-take-steps-protect-radioshack>
85. Smith A. *Record shares of Americans now own smartphones, have home broadband*. Pew Research Center, 2017, <http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/>
86. Tibken S. Smartphone sales fall for first time ever, says Gartner, 2018, <https://www.cnet.com/news/smartphone-sales-fell-for-the-first-time-ever-in-q4-apple-samsung-gartner/>
87. Bogost I. The wisdom of Nokia's dumbphone. *The Atlantic*, 2017, <https://www.theatlantic.com/technology/archive/2017/02/the-wisdom-of-the-dumbphone/518055/>
88. Juang M. As iPhone X raises the bar and price of smartphones, some consumers opt to switch to “dumbphones,” 2017, <https://www.cnn.com/2017/11/03/iphone-x-has-a-hefty-price-so-more-consumers-switch-to-dumbphones.html>