


Communication

# Privacy–Accuracy Consideration in Devices That Collect Sensor-Based Information

Lihid Dery <sup>1,2,\*</sup>  and Artyom Jelnov <sup>3,†</sup><sup>1</sup> Department of Industrial Engineering and Management, Ariel University, Ariel 40700, Israel<sup>2</sup> Ariel Cyber Innovation Center, Ariel University, Ariel 40700, Israel<sup>3</sup> Economics and Business, Ariel University, Ariel 40700, Israel; artyomj@ariel.ac.il

\* Correspondence: lihid@ariel.ac.il; Tel.: +972-74-723-3010

† The authors contributed equally to this work.

**Abstract:** Accurately tailored support such as advice or assistance can increase user satisfaction from interactions with smart devices; however, in order to achieve high accuracy, the device must obtain and exploit private user data and thus confidential user information might be jeopardized. We provide an analysis of this privacy–accuracy trade-off. We assume two positive correlations: a user’s utility from a device is positively correlated with the user’s privacy risk and also with the quality of the advice or assistance offered by the device. The extent of the privacy risk is unknown to the user. Thus, privacy concerned users might choose not to interact with devices they deem as unsafe. We suggest that at the first period of usage, the device should choose not to employ the full capability of its advice or assistance capabilities, since this may intimidate users from adopting it. Using three analytical propositions, we further offer an optimal policy for smart device exploitation of private data for the purpose of interactions with users.

**Keywords:** user–device interaction; privacy; smart devices; sensor-based information; privacy–accuracy trade-off

**Citation:** Dery, L.; Jelnov, A.Privacy–Accuracy Consideration in Devices That Collect Sensor-Based Information. *Sensors* **2021**, *21*, 4684. <https://doi.org/10.3390/s21144684>

Academic Editor: Antonio Fernández-Caballero

Received: 27 May 2021

Accepted: 26 June 2021

Published: 9 July 2021

**Publisher’s Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

Personal data can improve user experience as users receive personally tailored advice or assistance. For example, smart watch devices that track user movements suggest exercise when they detect the user is inactive for a long period of time [1]. Similarly, infrared sensors can detect falls and call for assistance [2]. However, in order to advise or assist, devices require access to personal information and these data require protection.

It is often unclear to the user what private information is collected, and if and how it is protected. Citing from a survey on the economics of privacy of [3]: “[Users’] ability to make informed decisions about their privacy is severely hindered because consumers are often in a position of imperfect or asymmetric information regarding when their data are collected, for what purposes, and with what consequences”.

The ability of individuals to manage privacy amid increasingly complex trade-offs is a problem, as faulty decisions may lead to privacy violations, which in turn incur various consequences. First, if information about users is leaked, it enables price discrimination. A second aspect is that of the violation of the user’s right to “peace and quiet”; for example, when receiving undesired adware (see [4]). Lastly, privacy violations might make it possible to sell user information to a third party.

We herein consider devices that employ user private information collected from sensors or devices provided with sensors. For example, by wearing a smart watch, the user shares information such as his location, heartbeat and movements. Using this information, the device is able to produce more accurate services. Users may be oblivious to the privacy risk at first. After an initial period in which they use the device, and once the device collects the data that are used to offer advice or assistance, the users may become aware of

the potential privacy risk. The users must trust the device to continue using it once they are aware of the privacy risk. When the device is not trusted, privacy risks and privacy violations may lead to users abandoning the device (also known as customer churn [5]). User perception of privacy and trust are therefore important [6–8].

**Contributions:** In this paper, we provide an analytical examination of how users' considerations of privacy risk affect their interactions with sensors and devices provided with sensors. We propose a model that shows that the user–device interaction has an interesting trend for users moderately concerned about their privacy. Nothing the device suggests will impact the very concerned or the very oblivious users, since they either do not trust the device with their information or are not concerned at all. However, the device's usage by users with a moderate privacy concern depends on how the users perceive the device's privacy risk. When the risk is not completely known to the users upfront, the users will use the device only if they trust it. With moderately concerned users, the device should choose not to employ the full capability of its advice or assistance capabilities, since this may intimidate the user from using it. Our results are not limited to any specific device and are generally true for any sensor or device provided with sensors that utilizes information where user privacy might be compromised.

The rest of the paper proceeds as follows. We begin with some background (Section 2). We then present a game-theoretical model and analytical results (Section 3). As some of the model is without mathematical proofs, we provide a numerical solution to the model (Section 4). We conclude with a discussion of our main findings (Section 5).

## 2. Related Work

As Acquisti et al. [3] have stated, “privacy is difficult to define”. In a similar manner, we focus on the informational dimension of privacy. i.e., the protection or sharing of personal data. There are two attitudes to the protection of private data: the protection is either handled by the device or by the user. When the privacy is left in the hands of the users, it is known as “privacy self-management” [9]. In some cases, install-time permissions provide users with control over their privacy as users are required to decide to whom to provide consent to collect, use and disclose their personal data [10]. In other cases, the users can choose between public and personal operation mode, or switch between these modes according to their activity context [11]. Often, users require assistance in privacy-related decisions [12].

Considerable research has focused on privacy from the device side, i.e., a technical perspective such as securing the channels over which information is sent [13] or collected [14]. Some researchers suggest zero-touch non-invasive systems where users do not need to engage with the system [15], while others secure the privacy of by-standers [16]. Interviews surveying how users perceive privacy of wearable devices conclude that there are a variety of user attitudes ranging from users who are not worried at all to users that are highly concerned for their privacy [17]. However, these studies do not consider actions following what users deem as a privacy risk nor do they present recommendations for devices.

John et al. [18] have experimentally shown that privacy-related cues affect the extent to which users are concerned about their privacy. Accordingly, previous research has emphasized the role of the clarity of the privacy policies on the user trust in the device or system used; changing the look of privacy policies makes online services appear more trustworthy [19]. Deciding which IOT-related devices are appropriate depends on the user familiarity more than it does on the privacy policy [20]. Similarly, [21] analyze the effects of both cognitive trust and emotional trust on the intention to opt in to health information exchanges and willingness to disclose health information.

We study scenarios where the users implicitly deduce the extent to which their private information is being analyzed, from the behavior of the device, as displayed in the advice or assistance the device offers. A user with a new smart watch might not bother to read the privacy policy of the smart watch's app. Nevertheless, after a short period of time, the user can easily deduce that they are being monitored, for example, when the watch suggests the

user should stretch, exercise or even breathe deeply [22]. It has been experimentally shown that smart watch usage is directly influenced by perceived usefulness and perceived privacy risk has a direct negative influence on the behavioral intention to use smart watches [23–25].

The above studies are experimental. For a general game theoretic model, where players exchange some information while being concerned about privacy, see [26] for example. In a more related context, Jullien et al. [27] discuss website users in situations where a website sells user information to third parties, which may lead to a good, a bad or a neutral experience for the users. In these situations, user vulnerability to a bad experience is unknown to the website. They consider a framework with two periods, where the users decide whether to stay with the website for the second period, depending on the first period outcome. In this work we implement the same two-period framework. However, Jullien et al. [27] study vulnerability as a property of the users, while we suggest examining risk as a property of the device.

In sum, previous studies that have focused on trust and privacy have shown that both have a direct effect on the usage of devices. However, these studies are of an experimental nature. In this paper we present a complementary analytical model that can explain the experimental results others have collected, support their claims and provide a better understanding of the privacy–accuracy trade-off for smart and sensor-based devices.

### 3. Model

We herein employ a game theoretic approach and examine a model containing a device with various possible degrees of privacy risks, and users that are uncertain as to the device privacy risk. In order to achieve high accuracy the device must obtain and exploit private user data and thus confidential user information might be jeopardized. We define accuracy as the degree of closeness of the advice or assistance offered by the device to the advice and assistance the user actually requires. We provide an analysis of this privacy–accuracy trade-off. We assume that a user’s utility from a device is positively correlated with:

1. The user’s privacy risk.
2. The advice or assistance offered by the device.

We consider an initial stage where the device only collects data, and a continuous stage where the device exploits the collected data.

For simplicity, we define two degrees of risks: (1) High risk, meaning that the user data are public or might be shared or sold to third parties and (2) Low risk, meaning that the user data are confidential. Let there be a user ( $C$ ) and a device ( $S$ ). The device has a high privacy risk ( $H$ ) with probability  $\pi$  and a low privacy risk ( $L$ ) with probability  $1 - \pi$ . We denote the device type by  $\rho = \{H, L\}$ . This  $\rho$  is unknown to the users. For convenience, all of the notation are found in Table 1.

Before usage, the user activates the device. Thus the user receives an initial signal of the device type, which is correct with probability  $1 - \epsilon$  and erroneous with probability  $\epsilon$ . Namely, if  $\rho = H$ , the user receives a signal  $h$  with probability  $1 - \epsilon$  and a signal  $l$  with probability  $\epsilon$ . If  $\rho = L$ , the user receives a signal  $l$  with probability  $1 - \epsilon$  and a signal  $h$  with probability  $\epsilon$ .

At **stage 1** (initial usage), the device chooses the accuracy level of its support algorithm (advice and/or assistance)  $q \in [0, 1]$ . We denote by  $q_H$  and  $q_L$  strategies chosen by the high type and the low type devices, respectively. The user receives adjusted support with probability  $P_a(q, \rho)$ . That is, the device’s support depends on the algorithm’s level of accuracy, and on the extent to which the device utilizes the private information it collected from the user. With a high risk device, the private information is more likely to be utilized, and vice versa. We assume that  $P_a(q, \rho)$  increases in  $q$  and for every  $q$ ,  $P_a(q, L) < P_a(q, H)$ . Denote by  $a$  the event “support is sent to the user”, and by  $\bar{a}$  the complementary event. Following  $a$ , the user’s utility is  $u_1 > 0$  and device’s utility is  $v_1 > 0$ . For  $\bar{a}$ , both the user and the device obtain utility 0. Following signal  $s \in \{h, l\}$  and event  $e \in \{a, \bar{a}\}$ , the user assigns a probability to the device being  $H$ :  $P(H|s, e)$

At **stage 2** (continuous usage), the user decides whether to keep using the device or to limit, reduce or abandon the device altogether. For simplicity, we look at two options: *leave* or *not leave*.

**Table 1.** List of notations in the model.

Notation	Description
$S$	device
$C$	user
$\rho$	device type (H-high risk; L-low risk)
$\pi$	prior probability of high risk
$s$	signal about device type
$\epsilon$	noise of the signal the user receives about device type
$q$	accuracy level of device support algorithm
$q_H$	accuracy level of high risk device support algorithm
$q_L$	accuracy level of low risk device support algorithm
$P_a(q, \rho)$	probability to receive adjusted support
$a, \bar{a}$	events "support sent/not sent to the user"
$P(H s, e)$	probability assigned by the user to the device being H
$P_b(\rho)$	probability of private information leaked
$u_1$	user utility from the adjusted support
$v_1$	device utility from the adjusted support
$u_b$	user utility if private information is leaked
$v_b$	device utility if private information is leaked
$u_H$	user utility at stage 2 from the high risk device, if no information is leaked
$u_L$	user's utility at stage 2 from the low risk device, if no information is leaked
$E_H^2$	high-risk device utility at stage 2
$E_L^2$	low-risk device utility at stage 2

If the user leaves, both user and device obtain a utility of 0. If the user does not leave, with probability  $P_b(\rho)$  ( $\rho$  is  $S$ 's type), the user's private information is leaked, exposing the user to possible damage. Let  $P_b(H) > P_b(L)$ . The utilities of the user and the device in this case are  $u_b < 0$  and  $v_b$ , respectively. With probability  $1 - P_b(\rho)$ , the user uses the device, and his/her utility is  $u_H$  and  $u_L$ , if  $\rho = H$  or  $\rho = L$ , respectively. We assume that  $u_H > u_L$ , namely, that the high type device has more value to the user, but this type has a higher privacy risk. We also assume that expected utilities of both  $H$  and  $L$  in stage 2 (denoted as  $E_H^2$  and  $E_L^2$ , respectively) are positive. The user's total utility is a total sum of the outcomes of stages 1 and 2.

We now turn to analyze if and when the users will abandon the device. If the potential damage  $|u_b|$  to the user is high, the user will leave the device, regardless of their belief of the device's type. The opposite is also true. If  $|u_b|$  is low, they will not leave regardless of their belief of the device type. For intermediate values of  $|u_b|$ , the user's strategy depends on the utility  $u_H$  of leaving a high-type device, when no damage is caused. If  $u_H$  is high, the user does not leave if they assign a sufficiently high probability to be a high-type device; however, if the utility  $u_H$  is relatively low, the user does not leave only if they assign a sufficiently low probability to the device being high type. Recall that the risk of being damaged by not abandoning the device is higher if the device type is H. This analysis

is formally stated in the following proposition. The proofs of all propositions appear in the Appendix A.

**Proposition 1.** Consider a Nash pure strategy equilibrium.

1. Let  $u_H > \frac{P_b(H)u_L(1-P_b(L))}{(1-P_b(H))P_b(L)}$ . Then in Nash equilibrium:
  - (a) If  $\frac{(1-P_b(H))u_H}{P_b(H)} < |u_b|$ , C prefers to leave at stage 2 for any  $P(H|s, e)$ .
  - (b) If  $|u_b| < \frac{(1-P_b(L))u_L}{P_b(L)}$ , C prefers not to leave at stage 2 for any  $P(H|s, e)$ .
  - (c) If  $\frac{(1-P_b(L))u_L}{P_b(L)} < |u_b| < \frac{(1-P_b(H))u_H}{P_b(H)}$ , there exists  $P_H^*$  such that C chooses not to leave iff  $P_H^* < P(H|s, e)$ .
2. Let  $u_H < \frac{P_b(H)u_L(1-P_b(L))}{(1-P_b(H))P_b(L)}$ . Then in Nash equilibrium:
  - (a) If  $|u_b| < \frac{(1-P_b(H))u_H}{P_b(H)}$ , C prefers not to leave at stage 2 for any  $P(H|s, e)$ .
  - (b) If  $\frac{(1-P_b(L))u_L}{P_b(L)} < |u_b|$ , C prefers to leave at stage 2 for any  $P(H|s, e)$ .
  - (c) If  $\frac{(1-P_b(H))u_H}{P_b(H)} < |u_b| < \frac{(1-P_b(L))u_L}{P_b(L)}$ , there exists  $P_H^*$  such that C chooses not to leave iff  $P(H|s, e) < P_H^*$ .

The next proposition states that at stage 1, if the signal about the device type is noisy (high  $\epsilon$ ), the device may choose not to offer maximal quality support ( $q_H = q_L = 1$ ). The reason being that when the quality is maximal, the probability of tailored support increases, and thus, the user's belief that the device type is  $H$  increases. At stage 2, if the benefit of  $H$  is sufficiently low (a low  $u_H$ ), the user may leave the device after receiving the tailored support.

**Proposition 2.** Suppose  $v_1 < E_H^2$  and  $v_1 < E_L^2$ . Let  $u_H < \frac{P_b(H)u_L(1-P_b(L))}{(1-P_b(H))P_b(L)}$ . Assume  $P_a(1, H)[1 - P_a(1, L)] > P_a(1, L)[1 - P_a(1, H)]$ . Then there is  $\epsilon < \frac{1}{2}$  and  $u_b$  such that  $q_H = q_L = 1$  is not a Nash equilibrium strategy of  $H$  and  $L$ .

When the signal about the device type is sufficiently precise, the user knows the device type with a high probability. Therefore, the user chooses whether to leave or not at stage 2 regardless of the outcomes of stage 1. In this case, the device chooses maximal quality (i.e., the best tailored support). Formally:

**Proposition 3.** For each  $u_b < 0$ , there is  $\epsilon^* > 0$  such that for all  $\epsilon < \epsilon^*$ ,  $q_H = q_L = 1$  is a unique equilibrium.

#### 4. Numerical Results

We present the following results using Monte Carlo simulations and computed with Matlab software. Consider a symmetric case, where the accuracy of the support algorithm ( $q$ ) is similar for both device types ( $q_H = q_L = q$ ). We assume that the probability to receive adjusted support depends on the accuracy level of the device's support algorithm; for high privacy risk devices it is two times more probable than for low privacy risk devices, i.e.,  $P_a(q, H) = q$  and  $P_a(q, L) = 0.5q$ . We further assume the following parameters are given as input:  $\pi = 0.5$  (equal prior to each type),  $u_1 = v_1 = 1$ ,  $u_L = 1$ ,  $u_H = 2$ ,  $E_L^2 = 2$ ;  $E_H^2 = 4$ ,  $u_b = -3$ ,  $P_b(L) = 0.2$  and  $P_b(H) = 0.8$ .

Note that these parameter values were intentionally chosen. With these values, if the device is of  $H$ -type, the expected utility of the user at stage 2 is negative:  $(1 - P_b(H))u_H + P_b(H)u_b = -2$ . If the device is of  $L$ -type, the expected utility of the user at stage 2 is positive:  $(1 - P_b(L))u_L + P_b(L)u_b = 0.2$ . Thus, these values present a non-trivial setting where it is unclear what the user should do. In contrast, when the expected user utility is negative for both high and low device types, the user has no incentive to use the device and will abandon it. Similarly, when the user-expected utility is positive for both device types,

the user will always use the device regardless of its type. Thus, the values were specifically chosen to accommodate the non-trivial case where the expected value is negative for one device type and positive for the other device type.

We performed the following procedure for different values of  $q$  ranging from 0 to 1. First we randomly generated two Bernoulli trials:

1. A Bernoulli trial for a signal on the device type  $s \in \{h, l\}$ .
2. A Bernoulli trial for the event that adjusted support is sent or not sent to the user  $e \in \{a, \bar{a}\}$ .

When the signal is  $a$  the device utility is  $v_1$ .

Then, we calculated the user belief of the device type (according to (A1)–(A4)). Next we calculated whether the user prefers to continue using the device in stage 2 (according to (A5)). If the user stays, the utility increases in  $E_H^2$  and  $E_L^2$  for devices with high ( $H$ ) and low ( $L$ ) privacy risks, respectively.

For each  $q \in \{0, 0.1, \dots, 1\}$  we ran this procedure for 10,000 trials, and then computed the average total utility (profit) of high and low-risk device types.

We present our numerical results in Figures 1–4. Each figure considers one of the following four signal accuracy levels  $\epsilon \in \{0.49, 0.3, 0.2, 0.05\}$ . Recall that a lower  $\epsilon$  means that the user has a better understanding of what the privacy risk is (at  $\epsilon = 0$  the user knows the risk for certain). The figures illustrate the average total profit (axis  $y$ ) as  $q$ , the accuracy of the support algorithm (axis  $x$ ) increases.

Figure 1 shows that when the signal on the device type is extremely noisy ( $\epsilon = 0.49$ ), both high and low device types profit from a higher accuracy strategy  $q$ , but the high-risk device type is better off if  $q = 0.9$ . In other words, both device types profit from sharing more accurate information and support with the user, but high privacy risk devices should be careful not to fully utilize all of their capabilities.

As user understanding of the privacy increases, i.e., as  $\epsilon$  decreases from  $\epsilon = 0.49$  in Figure 1 to  $\epsilon = 0.3$  and  $\epsilon = 0.2$  in Figures 2 and 3, respectively, the devices with a high privacy risk (type H) maximize their profit at lower accuracy values. This does not hold when the user knowledge of the device's risk is high ( $\epsilon = 0.05$  in Figure 4), since in this case, the users are aware of the privacy risk and thus the profit is maximized when the device outputs accurate support.

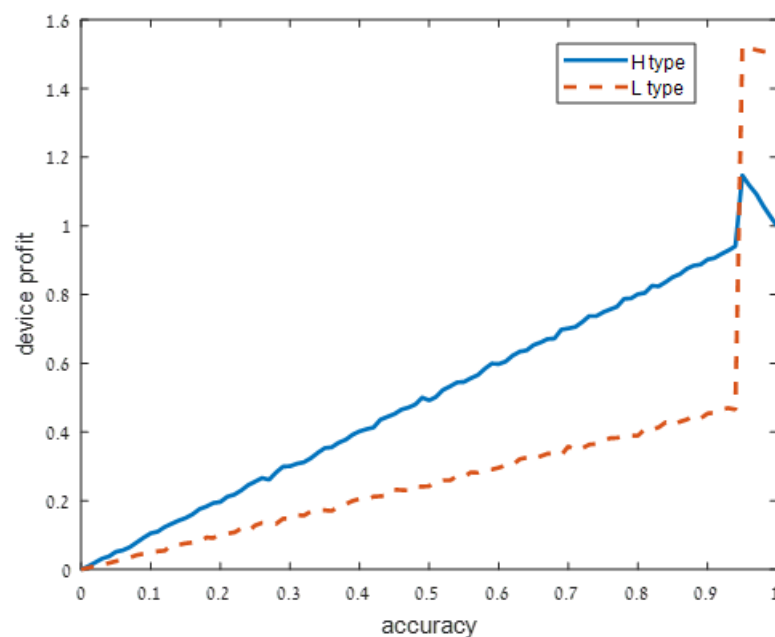


Figure 1. Extremely noisy signal:  $\epsilon = 0.49$ .

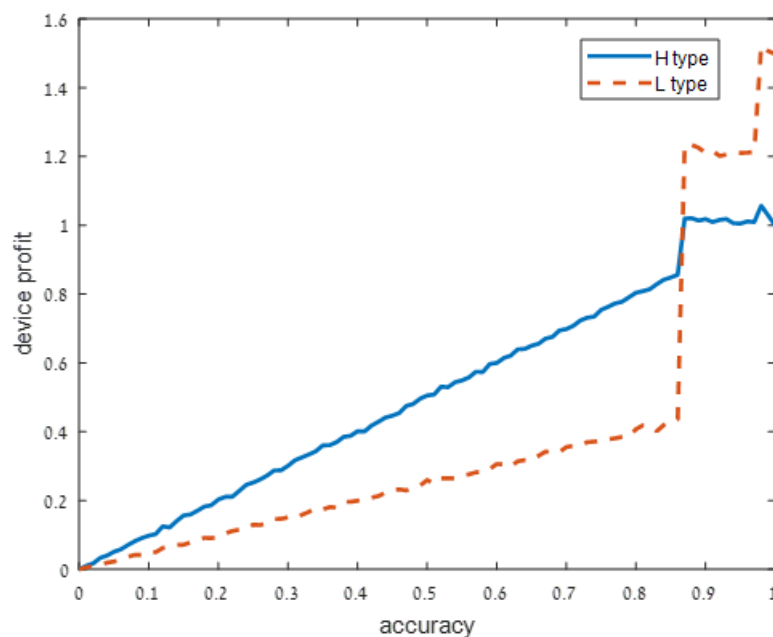


Figure 2. Moderately noisy signal:  $\epsilon = 0.3$ .

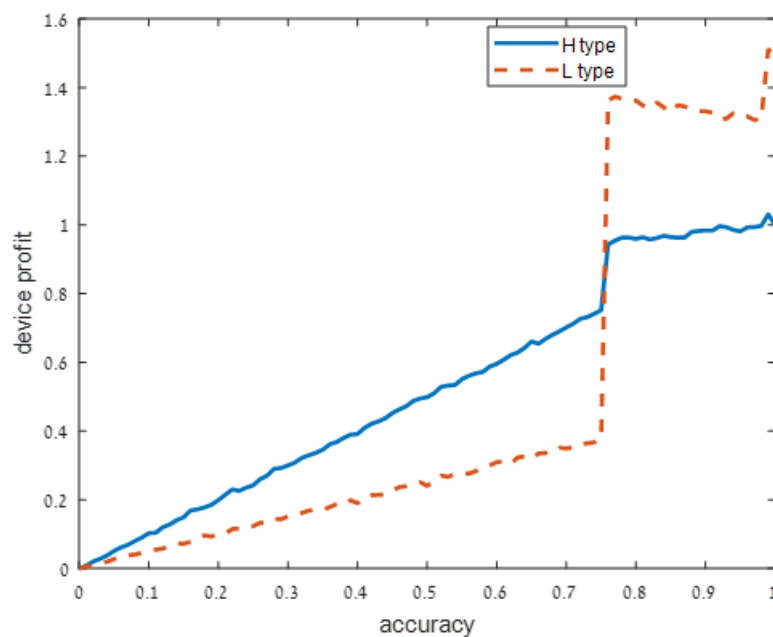


Figure 3. Moderately noisy signal:  $\epsilon = 0.2$ .

When the noise  $\epsilon$  is low, users know with high probability the type of device. It is not surprising then that the utility of the high-type device increases in  $q$ . It is more surprising that the utility of the low type device decreases in  $q$ . This may be explained by the fact that a negative effect of the adjusted support still persists (there is a small, but positive probability that following signal  $a$  the user will suspect that the device is of high risk). However, this effect is relatively weak.

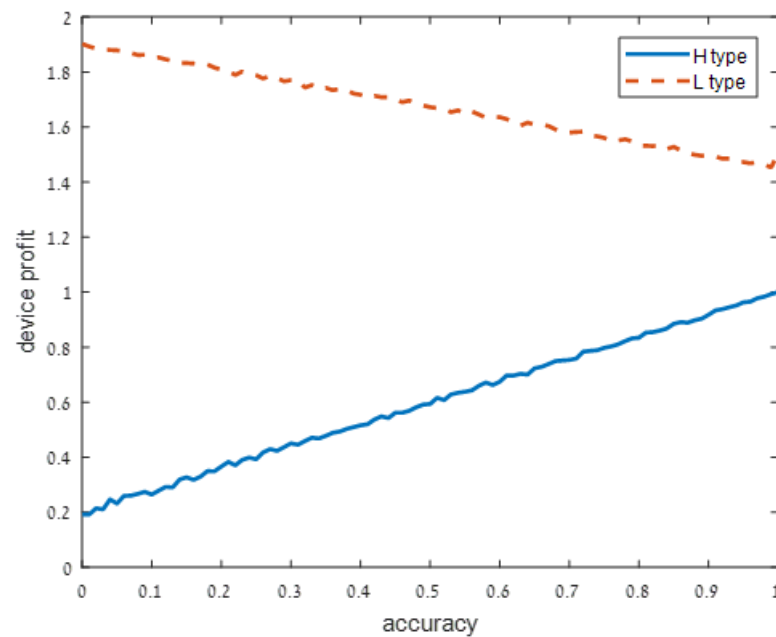


Figure 4. Low noise:  $\epsilon = 0.05$ .

## 5. Discussion

We analyzed how privacy risk considerations affect the decisions of both the devices and the users. Our main finding herein is that when the device's privacy risk is unknown to the users it might be inefficient for the device to exploit its sensing technology, since this may lead users to abandon the device.

Specifically, based on our three analytical propositions, we suggest the following for optimal acceptance of devices provided with sensors when the privacy risk is unknown to the users. Our suggestions focus on the communication between the device and the user, specifically on the device feedback policy. These suggestions do not depend on technical characteristics of device, e.g., the sensor's accuracy and cost.

1. **Assure low risk**—Convincing the user that the device has a low privacy risk for them is of urgent importance. Risk-concerned users who are not convinced will quickly abandon the device. For example, publish a clear and easy to understand privacy policy.
2. **Limit initial accurate feedback**—Accurate advice and assistance might be the most intuitive way to exhibit the device's usefulness. However, at the first usage period the device should do so with caution. A risk-concerned user might abandon the device due to accurate feedback. So this feedback should sometimes be withheld. This is because, from accurate feedback, the user concludes that their privacy is being compromised.
3. **Second stage accurate feedback is welcome**—Once the user is aware of the privacy risk, and given that they did not abandon the device in the first usage period, they will probably not abandon the device due to privacy concerns later on. If users do not identify a risk, they will keep using the device.

Each of these propositions is both grounded analytically, and also intuitive to understand. However, applying the three of them in practice is not trivial. In future work we plan to apply these recommendations to a wearable device.

**Author Contributions:** Conceptualization, L.D. and A.J.; methodology, L.D. and A.J.; formal analysis, L.D. and A.J.; investigation, L.D. and A.J.; resources, L.D. and A.J.; writing—original draft preparation, L.D. and A.J.; writing—review and editing, L.D. and A.J.; project administration, L.D. and A.J. Both authors have read and agreed to the published version of the manuscript.



**Funding:** Lihi Dery was supported by the Ariel Cyber Innovation Center in conjunction with the Israel National Cyber Directorate in the Prime Minister’s Office. Artyom Jelnov was supported by the Heth Academic Center for research of competition and regulation.

**Conflicts of Interest:** The authors declare no conflict of interest.

## Appendix A

**Proof of Proposition 1.** Following signal  $h$  and event  $a$ , C’s belief that S is H is

$$P(H|h, a) = \frac{\pi(1 - \epsilon)P_a(q_h, H)}{\pi(1 - \epsilon)P_a(q_h, H) + (1 - \pi)\epsilon P_a(q_L, L)}. \quad (\text{A1})$$

Following signal  $h$  and event  $\bar{a}$ , C’s belief that S is H is

$$P(H|h, \bar{a}) = \frac{\pi(1 - \epsilon)(1 - P_a(q_h, H))}{\pi(1 - \epsilon)(1 - P_a(q_h, H)) + (1 - \pi)\epsilon(1 - P_a(q_L, L))}. \quad (\text{A2})$$

Following signal  $l$  and event  $a$ , C’s belief that S is H is

$$P(H|l, a) = \frac{\pi\epsilon P_a(q_h, H)}{\pi\epsilon P_a(q_h, H) + (1 - \pi)(1 - \epsilon)P_a(q_L, L)}. \quad (\text{A3})$$

Following signal  $l$  and event  $\bar{a}$ , C’s belief that S is H is

$$P(H|l, \bar{a}) = \frac{\pi\epsilon(1 - P_a(q_h, H))}{\pi\epsilon(1 - P_a(q_h, H)) + (1 - \pi)(1 - \epsilon)(1 - P_a(q_L, L))}. \quad (\text{A4})$$

Let  $s \in \{l, h\}$  be a signal received by C about S’s type, and  $e \in \{a, \bar{a}\}$  be the event outcome of stage 1. C prefers not to leave at stage 2 iff

$$P(H|s, e)[P_b(H)u_b + (1 - P_b(H))u_H] + (1 - P(H|s, e))[P_b(L)u_b + (1 - P_b(L))u_L] \geq 0, \quad (\text{A5})$$

which is equivalent to

$$-u_b \leq \frac{P(H|s, e)[(1 - P_b(H))u_H - (1 - P_b(L))u_L] + (1 - P_b(L))u_L}{P(H|s, e)[P_b(H) - P_b(L)] + P_b(L)}. \quad (\text{A6})$$

Let  $u_H > \frac{P_b(H)u_L(1 - P_b(L))}{(1 - P_b(H))P_b(L)}$ . Then the right-hand side of (A6) increases in  $P(H|s, e)$  and its maximum, obtained for  $P(H|s, e) = 1$ , is

$$\frac{(1 - P_b(H))u_H}{P_b(H)},$$

and the minimum (at  $P(H|s, e) = 0$ ) is

$$\frac{(1 - P_b(L))u_L}{P_b(L)}.$$

Therefore, for  $\frac{(1 - P_b(H))u_H}{P_b(H)} < -u_b$ , C prefers to leave at stage 2 for any  $P(H|s, e)$ . For  $-u_b < \frac{(1 - P_b(L))u_L}{P_b(L)}$ , C prefers not to leave at stage 2 for any  $P(H|s, e)$ . If  $\frac{(1 - P_b(L))u_L}{P_b(L)} < -u_b < \frac{(1 - P_b(H))u_H}{P_b(H)}$ , there exists  $P_H^*$  such that (A6) holds iff  $P_H^* \leq P(H|s, e)$ .

Next, suppose  $u_H < \frac{P_b(H)u_L(1 - P_b(L))}{(1 - P_b(H))P_b(L)}$ . Then the right-hand side of (A6) decreases in  $P(H|s, e)$ . For  $\frac{(1 - P_b(H))u_H}{P_b(H)} > -u_b$ , C prefers not to leave at stage 2 for any  $P(H|s, e)$ . For  $-u_b > \frac{(1 - P_b(L))u_L}{P_b(L)}$ , C prefers to leave for any  $P(H|s, e)$ . If  $\frac{(1 - P_b(L))u_L}{P_b(L)} > -u_b > \frac{(1 - P_b(H))u_H}{P_b(H)}$ , there exists  $P_H^*$  such that (A6) holds iff  $P_H^* \geq P(H|s, e)$ .  $\square$

**Proof of Proposition 2.** Suppose by contrary  $q_H = q_L = 1$  in equilibrium. By assumption  $P_a(1, H)[1 - P_a(1, L)] > P_a(1, L)[1 - P_a(1, H)]$ , thus by continuity there is  $\epsilon < \frac{1}{2}$  such that  $\epsilon^2 P_a(1, H)[1 - P_a(1, L)] > (1 - \epsilon)^2 P_a(1, L)[1 - P_a(1, H)]$ , and by (A2) and (A3),  $\bar{P}(H|h, \bar{a}) < P(H|l, a)$ .

By (A1)–(A4), for  $\epsilon < \frac{1}{2}$ ,  $P(H|h, e) > P(H|l, e)$ ,  $s = a, \bar{a}$ . To summarize,

$$P(H|l, \bar{a}) < P(H|h, \bar{a}) < P(H|l, a) < P(H|h, a). \quad (\text{A7})$$

Let  $RHS(P(H|s, e))$  be the right-hand side of (A6) for given  $P(H|s, e)$ . For  $u_H < \frac{P_b(H)u_L(1-P_b(L))}{(1-P_b(H))P_b(L)}$ ,  $RHS(P(H|s, e))$  decreases in  $P(H|s, e)$ . Therefore,

$$RHS(P(H|l, \bar{a})) > RHS(P(H|h, \bar{a})) > RHS(P(H|l, a)) > RHS(P(H|h, a)). \quad (\text{A8})$$

By (A6) and by (A8), if  $RHS(P(H|l, a)) < |u_b| < RHS(P(H|h, \bar{a}))$ , for both  $h$  and  $l$  signals C chooses not to leave following  $\bar{a}$  and to leave following  $a$ . The expected utility of  $H$  is therefore

$$P_a(1, H)v_1 + (1 - P_a(1, H))E_H^2,$$

and by  $v_1 < E_H^2$ , and by being  $P_a(q_H, H)$  decreasing in  $q_H$ ,  $H$  is better off by deviating to  $q_H < 1$ . Similarly,  $L$  is better off by deviating to  $q_L < 1$ , contradiction.  $\square$

**Proof of Proposition 3.** By (A1)–(A4), for every  $e \in \{a, \bar{a}\}$ ,  $P(H|h, e) \rightarrow 1$  and  $P(H|l, e) \rightarrow 0$  as  $\epsilon \rightarrow 0$ . Therefore, the right-hand side of (A6) converges to a constant independent on  $a$  or  $\bar{a}$ , and C chooses to leave or not to leave at stage 2, independent on even  $a$  or  $\bar{a}$ . Thus, both  $H$  and  $L$  maximize their payoffs at stage 1, which are maximized for  $q_H = q_L = 1$ .  $\square$

## References

1. Reeder, B.; David, A. Health at hand: A systematic review of smart watch uses for health and wellness. *J. Biomed. Inform.* **2016**, *63*, 269–276. [CrossRef] [PubMed]
2. Tao, S.; Kudo, M.; Nonaka, H. Privacy-preserved behavior analysis and fall detection by an infrared ceiling sensor network. *Sensors* **2012**, *12*, 16920–16936. [CrossRef] [PubMed]
3. Acquisti, A.; Taylor, C.; Wagman, L. The economics of privacy. *J. Econ. Lit.* **2016**, *54*, 442–492. [CrossRef]
4. Spiegel, Y. Commercial software, adware, and consumer privacy. *Int. J. Ind. Organ.* **2013**, *31*, 702–713. [CrossRef]
5. Munia, A.; Nicotra, M.; Romano, M. Big Data, Predictive Marketing and Churn Management in the IoT Era. In *The Internet of Things Entrepreneurial Ecosystems*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 75–93.
6. Chang, Y.; Wong, S.F.; Libaque-Saenz, C.F.; Lee, H. The role of privacy policy on consumers' perceived privacy. *Gov. Inf. Q.* **2018**, *35*, 445–459. [CrossRef]
7. Balapour, A.; Nikkiah, H.R.; Sabherwal, R. Mobile application security: Role of perceived privacy as the predictor of security perceptions. *Int. J. Inf. Manag.* **2020**, *52*, 102063. [CrossRef]
8. Mutimukwe, C.; Kolkowska, E.; Grönlund, Å. Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Gov. Inf. Q.* **2020**, *37*, 101413. [CrossRef]
9. Solove, D.J. Introduction: Privacy self-management and the consent dilemma. *Harvard Law Rev.* **2012**, *126*, 1880.
10. Felt, A.P.; Chin, E.; Hanna, S.; Song, D.; Wagner, D. Android permissions demystified. In Proceedings of the 18th ACM conference on Computer and Communications Security, Chicago, IL, USA, 17–21 October 2011; ACM: New York, NY, USA, 2011; pp. 627–638.
11. Yan, H.; Li, X.; Wang, Y.; Jia, C. Centralized duplicate removal video storage system with privacy preservation in iot. *Sensors* **2018**, *18*, 1814. [CrossRef] [PubMed]
12. Acquisti, A.; Adjerid, I.; Balebako, R.; Brandimarte, L.; Cranor, L.F.; Komanduri, S.; Leon, P.G.; Sadeh, N.; Schaub, F.; Sleeper, M.; et al. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Comput. Surv. (CSUR)* **2017**, *50*, 44. [CrossRef]
13. Hamza, R.; Yan, Z.; Muhammad, K.; Bellavista, P.; Titouna, F. A privacy-preserving cryptosystem for IoT E-healthcare. *Inf. Sci.* **2020**, *527*, 493–510. [CrossRef]
14. Kim, J.W.; Lim, J.H.; Moon, S.M.; Jang, B. Collecting health lifelog data from smartwatch users in a privacy-preserving manner. *IEEE Trans. Consum. Electron.* **2019**, *65*, 369–378. [CrossRef]
15. Grgurić, A.; Mošmondor, M.; Huljenić, D. The SmartHabits: An intelligent privacy-aware home care assistance system. *Sensors* **2019**, *19*, 907. [CrossRef] [PubMed]
16. Perez, A.J.; Zeadally, S.; Griffith, S.; Garcia, L.Y.M.; Mouloud, J.A. A User Study of a Wearable System to Enhance Bystanders' Facial Privacy. *IoT* **2020**, *1*, 198–217. [CrossRef]

17. Lowens, B.; Motti, V.G.; Caine, K. Wearable privacy: Skeletons in the data closet. In Proceedings of the 2017 IEEE International Conference on Healthcare Informatics (ICHI), Park City, UT, USA, 23–26 August 2017; IEEE: New York, NY, USA, 2017; pp. 295–304.
18. John, L.K.; Acquisti, A.; Loewenstein, G. Strangers on a plane: Context-dependent willingness to divulge sensitive information. *J. Consum. Res.* **2011**, *37*, 858–873. [[CrossRef](#)]
19. Aïmeur, E.; Lawani, O.; Dalkir, K. When changing the look of privacy policies affects user trust: An experimental study. *Comput. Hum. Behav.* **2016**, *58*, 368–379. [[CrossRef](#)]
20. Kaupins, G.; Coco, M. Perceptions of internet-of-things surveillance by human resource managers. *SAM Adv. Manag. J.* **2017**, *82*, 53.
21. Esmaeilzadeh, P. *The Impacts of the Privacy Policy on Individual Trust in Health Information Exchanges (HIEs)*; Internet Research: Toulouse, France, 2020. [[CrossRef](#)]
22. Hatamian, M.; Momen, N.; Fritsch, L.; Rannenber, K. A multilateral privacy impact analysis method for android apps. In *Annual Privacy Forum*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 87–106.
23. Ernst, C.P.H.; Ernst, A.W. The Influence of Privacy Risk on Smartwatch Usage. Available online: [https://www.frankfurt-university.de/fileadmin/standard/Hochschule/Fachbereich\\_3/Kontakt/Professor\\_inn\\_en/Ernst/Publikationen/The\\_Influence\\_of\\_Privacy\\_Risk\\_on\\_Smartwatch\\_Usage.pdf](https://www.frankfurt-university.de/fileadmin/standard/Hochschule/Fachbereich_3/Kontakt/Professor_inn_en/Ernst/Publikationen/The_Influence_of_Privacy_Risk_on_Smartwatch_Usage.pdf) (accessed on 2 June 2021).
24. Lee, J.M.; Rha, J.Y. Personalization–privacy paradox and consumer conflict with the use of location-based mobile commerce. *Comput. Hum. Behav.* **2016**, *63*, 453–462. [[CrossRef](#)]
25. Kang, H.; Jung, E.H. The Smart Wearables-Privacy Paradox: A Cluster Analysis of Smartwatch Users. Available online: <https://www.tandfonline.com/doi/abs/10.1080/0144929X.2020.1778787?journalCode=tbit20> (accessed on 2 June 2021).
26. Dziuda, W.; Gradwohl, R. Achieving cooperation under privacy concerns. *Am. Econ. J. Microeconomics* **2015**, *7*, 142–173. [[CrossRef](#)]
27. Jullien, B.; Lefouili, Y.; Riordan, M. *Privacy Protection and Consumer Retention*; Technical Report; Toulouse School of Economics (TSE): Toulouse, France, 2018.