Privacy Implications of Wearable Health Devices

Greig Paul
University of Strathclyde
Department of Electronic & Electrical Engineering
Glasgow, United Kingdom
greig.paul@strath.ac.uk

James Irvine
University of Strathclyde
Department of Electronic & Electrical Engineering
Glasgow, United Kingdom
j.m.irvine@strath.ac.uk

ABSTRACT
With the recent rise in popularity of wearable personal health monitoring devices, a number of concerns regarding user privacy are raised, specifically with regard to how the providers of these devices make use of the data obtained from these devices, and the protections that user data enjoys. With waterproof monitors intended to be worn 24 hours per day, and companion smartphone applications able to offer analysis and sharing of activity data, we investigate and compare the privacy policies of four services, and the extent to which these services protect user privacy, as we find these services do not fall within the scope of existing legislation regarding the privacy of health data. We then present a set of criteria which would preserve user privacy, and avoid the concerns identified within the policies of the services investigated.

Categories and Subject Descriptors
K.4.1 [**Computers and Society**]: Public Policy Issues—*Privacy*

General Terms
Security, Legal Aspects

Keywords
Health monitoring, privacy, security, wearables

1. INTRODUCTION
As smartphone ownership levels rise, a growing market in user-operated wearable health-monitoring technology has emerged. While wearable health sensors have been used by doctors and medical professionals for many years, the latest wearable health sensors are marketed to consumers, promising lifestyle and health analysis. The majority of these services upload raw sensor data from the health sensor to the service provider servers, using a smartphone for transmission of data, and to display measurements and analysis. With one centralised location for all service users' health data, measures taken to preserve user privacy and security are especially important, given the health-oriented nature of the data. The significance of user privacy and data security for users of health applications was highlighted in the survey conducted in [17].

In common with almost every website, these services feature terms and conditions, as well as dedicated privacy policies. These policies, which typically inform users of their rights, and the extent to which the company may access and share their data, were found in some cases to result in the company claiming rights to the user's own health data, and in one case to even claim ownership of the user's raw health data.

By investigating the types of data collected by each of these services, as well as their privacy policies for handling such data, it is possible to identify a number of privacy risks for users. which users of these kinds of emerging services may be unwittingly exposing themselves to, and the possible consequences of these.

2. PRODUCT OVERVIEW
For the purpose of this investigation, four different health monitoring services were investigated. The services selected are all marketed directly to the end-user, and all were readily available for purchase. Each service provider offers a version of their service free for buyers of their hardware monitors. The services investigated in this article were Fitbit, Jawbone, Nike+ and BASIS.

All of these services required registration for an online account in order to use the wearable device - all information recorded by the device was then uploaded to the provider's online service. After logging into this account, analysis of the data is offered to the user via a website or smartphone application.

Each of these services presented at least two policies covering user privacy, and in the following sections, these policies were investigated for each service, with potential user privacy concerns are discussed.

2.1 Fitbit
The Fitbit website terms and conditions state that a user agrees to allow Fitbit to "use and commercially exploit any text, photographs or other data and information you submit to the Fitbit Services", and that users "waive any rights of publicity and privacy" to any data they submit to the

service. [7] Given that user health data is submitted to the service through a mobile application over the internet, this would count as "other data", and therefore result in the user having no right to privacy over any of their own health data recorded by a Fitbit device.

In the event of a Fitbit user terminating their account, Fitbit's privacy policy states that all personally identifiable information will be removed, but that Fitbit may continue to use "de-identified and anonymized historical data" from their use of Fitbit products. [8] Section 5 discusses the risks to user privacy posed by advances in de-anonymisation techniques.

In order to register for a Fitbit account, it is necessary for a user to supply accurate and complete personal information, and Fitbit state they may suspend accounts of users who appear to have inaccurate or incomplete registration data supplied. [7] This would appear to prevent a user from making use of a pseudonym or other privacy-preserving false identity. Such an approach was recommended by Andy Smith, internet security chief at the UK Cabinet Office, who stated that "When you put information on the internet do not use your real name, your real data of birth", "because it can be used against you" (by criminals). [21]

Fitbit also state in their privacy policy that they record GPS location data unless users opt out. [8]

2.2 Jawbone

The Jawbone privacy policy states firstly that all Jawbone users are listed in a publicly searchable directory, containing their name and profile photograph. The policy does not refer to any ability for users to opt out of being displayed in this directory. Additionally. Jawbone state that they upload the contacts list, and calendar data, from smartphones running their app. [11] While user contacts are gathered for the purpose of finding friends also using the service, this offers no explanation as to why a user's calendar is uploaded.

Jawbone also state that they "may get information about you from other sources" and "add this information to the information we have already collected from you in order to improve the products and services". [11] There are no limitations given as to the sources of this information, or the kind of information which may be included, or even the purpose for which this information would be used.

In addition, Jawbone also collect a user's full name, photo, gender, height, weight and date of birth, as well as the GPS location of users, via their mobile phone. [11]

The Jawbone privacy policy states that "You can delete any activity or sleep tracked in the UP band via the Help screen in the UP app. You can erase band data by..." [11]. There is no indication of whether this data is also erased on the servers, or if it only applies to the local data stored on the monitoring device.

2.3 Nike+

The Nike+ Fuelband privacy policy states that it logs and stores the GPS location of users on its servers, and that it collects information from "public sources" and "third parties". Again, there was no information as to the kinds of sources used, nor the intended purpose of storing such information. Users of the Nike+ service are given the ability to delete their data at any time. [14]

2.4 BASIS

The privacy policy for the BASIS watch service states that "all biometric data shall remain the sole and exclusive property of BASIS Science, Inc." BASIS define biometric data as being time-stamped heart rate, skin temperature, ambient temperature, galvanic skin response, and acceleromter measurement. BASIS also reserve the right to make commercial use of this data, such as selling it in aggregate form, for marketing and sales use, and that BASIS may retain this data as they deem necessary or appropriate. As such, it appears that users have no right to have their historical data removed from the service at a point in future. [2]

The BASIS terms and conditions also require that users register and provide "accurate and complete" registration information, and keep it updated. This means that were users to follow Andy Smith's advice about using false identifiers they would contravene the terms and conditions.

The terms and conditions state that "we keep all your information confidential and encrypted" [3], which is in direct contradiction to their privacy policy, which states that "we do not encrypt data in our database". [2]

BASIS also state that "We may access the Biometric Data of a user to provide customer support for such user, subject to our internal BASIS Security Policy". Unfortunately, no details are given of this security policy, and therefore it is not possible to ascertain what level of privacy can be expected of data uploaded to the service. [2]

3. GENERAL CONCERNS

From our analysis of the privacy policies and other terms and conditions of these services, a number of more general privacy concerns were identified. These are not unique to wearable health montoring devices, and a number of these are discussed in [22]. In [9], the importance of preserving user privacy in e-health systems is discussed in greater detail. In particular, within the context of e-health services, Hong et al. state that "people who use the internet for health-related reasons have the right to expect that personal data they provide will be kept confidential". A natural question as a result of such research is as to whether or not the data captured from a wearable health-monitoring device constitutes "personal data" due to its inherently private nature, even though it may in itself not necessarily contain identifying information.

3.1 Data Ownership

As discussed in [6], medical-related data poses a number of questions, particularly with regards to ownership. In the case of BASIS, their privacy policy asserted ownership of data gathered from users, as their "sole and exclusive property". None of the other four services reviewed made a claim to user data in this manner, although Fitbit reserved the right to "use and commercially exploit" all data submitted by users to their service, with no right to privacy. [8]

3.2 Classification of Data

Within the United States, HIPAA (Health Information Portability and Accountability Act) legislation [1] offers privacy protection for health data. As discussed in [18], two main criteria are used when determining whether or not data is protected by this legislation. The first is whether or not the company processing the data is a "covered entity" (these include "healthcare providers, health plans, and healthcare clearinghouses"). The second is as to whether or not the data in question is individually identifiable health information, since non-identifiable (or anonymised) data is not protected by HIPAA legislation. As stated in [18], data is only classified as de-identified when there is no information that can reasonably be used to identify the individual in question. Simply removing the name is not sufficient, if the individual could be identified through other means. This is discussed in section 5.

The only service to make reference to HIPAA legislation was BASIS, which stated in its privacy policy that it "is not a "covered entity" or "business associate" under the Health Insurance Portability and Accountability Act...", and that therefore the legislation does not cover data sent to their service. [2]

As discussed in [19], from the perspective of wearable health monitors in a clinical situation, in the event of personal or health data being compromised, it is unclear as to whether or not the doctor, or the wearable device service provider, would be liable. While the services investigated here are for use by individuals, rather than medical professionals, and as such are not covered by HIPAA, [4] offers an analysis, highlighting that the data produced by a user-operated wearable health monitoring device would not be HIPAA-protected. If however, that data was gathered by a healthcare provider, or indeed even transferred to a healthcare provider, it would itself then become HIPAA-protected information, as it would be "considered a part of the patient's health records".

3.3 Jurasdiction of Data Storage

All four services studied stated that user data would be stored outwith the European Union (which has specific and often stronger protections for user private data) [20]. Nike+ did state that they would not transfer user data outwith the Nike group, unless necessary for a service provider (like shipping or payment processing). [14]

Also of relevance is the Safe Harbor agreement, between the United States and European Union, which is a voluntary process through which US-based companies with a presence in Europe can self-certify that they meet the fundamental privacy requirements required by the EU. These fundamental requirements state that:

"Under the directive, companies must allow consumers to access their data, know where it originated, correct and update information, withhold personal data from unauthorized uses, and take legal recourse for unlawful processing of personal data" [13]

Both Nike+ and Fitbit state that they comply with the Safe Harbor agreement. Jawbone and BASIS made no statement regarding the compliance of their services with Safe Harbor.

4. ABILITY TO DELETE DATA

Of the services reviewed, only Nike+ had a policy which stated users may remove all data which was stored about them. [15] While Jawbone stated that users may delete activity or sleep information tracked via the app, it did not make clear whether or not such data would be removed from their servers, or just the wearable device itself. [11] There was also no statement made as to users' ability to remove the contacts or calendar data uploaded by the Jawbone service, as discussed in section 2.2.

BASIS did not make any right to remove all user data clear, although their policy details may have precluded such a feature, given BASIS claims ownership over user health data (as discussed in section 2.4).

Fitbit state that personally identifiable information will be removed from accounts which are terminated, but that they may continue to use de-identified data already collected (as discussed in section 2.1).

As discussed in [20], the US FTC (Federal Trade Commission) expects that commercial websites offer customers the ability to correct or delete information.

5. RISK OF FUTURE REIDENTIFICATION

A trend we identified in the privacy policies of the services investigated was to permit "anonymised" or de-identified data to be used for statistics or further analysis, even after a user had ceased using a service. One potential well-documented risk of such procedures is that of re-identification, whereby previously anonymised data can be re-associated with the identity of the individual it was captured from. Montjoye et al. demonstrated in [5] the ease with which location data was used to identify an individual, even with coarse datasets, or with sporadic sampling intervals. Ohm [16] concluded that reidentification of anonymised data is a significant concern, and that "data can be either useful or perfectly anonymous, but never both", and that many laws offer exemptions for anonymised data, which as discussed by Ohm, could be reidentified, potentially putting the privacy of users at risk.

6. SERVICE PROVIDER POLICY CHANGES

Of the four services investigated, none made a firm committment to proactively notify users clearly of any substantial privacy policy changes. Fitbit's privacy policy contains a date of last modification, but states that changes to the policy take effect "immediately upon posting", meaning a change to the policy would affect a user no longer making use of the service, and that they may not even be made aware of the change to the policy which governs the use of their historically gathered personal data.

Jawbone's privacy policy contained a notice that the policy may be updated, and contains a date of last modification. There was no statement of when these updated terms and conditions would apply. The Nike+ privacy policy likewise contained a date of last modification, and stated that updated versions of the policy would be posted on the website, and that users are "advised to regularly check whether our privacy policy has changed". [15] Once again, neither of these policies would necessarily ensure users were aware of the changes to the policy.

BASIS stated that they may modify their privacy policy at any time, and will provide "prominent notice" by posting an updated copy to their support page, and that users should review this page to see any changes. The date of last modification is given on the policy.

The ease with which these privacy policies may be modified is not unique to wearable health monitoring services - [12] carried out an informal review of 30 websites, and found that none committed to directly notifying users of changes to their policy, instead leaving the responsibility on users to regularly check the privacy policy of each service they use. Despite this being a universal trend among internet services, it is clear that any of the wearable health monitoring services investigated here could effectively change their privacy policy without users realistically becoming aware of the change. Even if they were aware, only Nike+ stated they offered users a means to remove all data held in their account, and a future revision of the policy could theoretically prevent users from removing their own data, in line with the policies Fitbit and BASIS have in place.

7. COMPARISON TABLE

By way of comparison of the privacy features offered by each service, table 7 was created. For each service, the privacy policy and terms and conditions of use were used to reflect each category. An overall privacy score was calculated as the sum of all positive comparison results. Each category was equally weighted due to the subjectivity of user privacy priorities.

8. A MODEL TO PRESERVE PRIVACY

The four services investigated make significant use of internet-connectivity, and do not permit users to make use of the wearable health monitor offline, meaning that users have no ability to use the product without agreeing to the service privacy policies. In line with our findings, as summarised in table 7 previously, we propose a model for a privacy-preserving wearable health monitoring platform.

An ideal platform for wearable health monitoring, from a privacy perspective, would be capable of operating fully offline, with no requirement for user registration. Many of the concerns identified with the four services investigated were directly as a result of users being required to transmit their data to cloud infrastructure operated by the service provider. Given the increases in mobile device storage capacities, and the ever-decreasing costs of storage, a health monitoring platform where data is locally stored and analysed on a user's smartphone would be practical, and also alleviate concerns of data being held and processed by third parties.

Where cloud-based features were used, these would be optional, and would inform users clearly of precisely what data would be made available, and to whom, by using the feature, before confirming the user wished to upload that data, to ensure informed consent is given for all health data transfers. No supplementary data should be gathered from the user's device in this process.

To ensure user confidence in the service, and ensure users' rights to erase their data are upheld, any internet-based portions of such a service should have a clear means through which all user-submitted data (and resulting analysis of such data) can be permanently erased from the provider's systems. Likewise, to minimise the risk to user's personally identifiable information (PII), as little PII should be requested, and stored, as possible. For example, users should not be required to enter their full name, or any other identifying information, given alternative unique identifiers could be used (such as account numbers, or user-selected pseudonyms). Likewise, rather than asking users for their date of birth, users could be asked to supply a binned age group (for the purpose of making calculations related to health matters), such as 40 to 45.

In order to prevent user data from being exposed to those operating the service, the data stored by the provider should be encrypted at a per-user level, in order to deliver a "zero-knowledge" service, whereby the operator of the service cannot access user data, as it is encrypted by a key derived from a password known only to the user. This is demonstrated, in the context of preservation of user privacy in location-based services, in [10].

Such a product, while not inkeeping with the centralised cloud service philosophy, would ensure that user privacy was preserved, when dealing with sensitive data, specifically that from their wearable health sensors, which users have an expectation to be kept private and secure. [9]

Similarly, in order to ensure that users are not adversely affected by any future policy updates, users would be proactively notified by email if the privacy policy were to be updated in the future. The updated policy would take effect from a date in the future, offering users a period of time in which they may remove their account from the service, along with all their data, if they do not agree to the updated policy, and would prefer to have their data removed.

9. CONCLUSIONS

In this evaluation of the privacy policies in place for four services in the emerging and growing field of wearable health monitoring systems, it is clear that there are a number of considerations to privacy which users may not be aware of. Despite each service providing at least two policies covering privacy or security matters, these policies appear unlikely to be read frequently by users - in the case of one service, their policies were directly contradictory as to whether or not user data was encrypted on their servers. These policies were last modified in November 2012, indicating that this contradiction has been in place for at least 18 months without being rectified.

Two services investigated appeared to claim sufficient rights to data submitted by users that the operators would be able to retain recorded health data indefinitely, without the subject (the end user) being able to request its removal. In one instance, the service provider claimed full ownership of data recorded from the user's wearable health sensor. Another service operator stated that users had no right to privacy to any data they provided the service, perhaps concerning in the context of a wearable health monitoring device.

Two of the services investigated also made no claim to com-

Table 1: Comparison of Service Privacy Policies

	Fitbit	Jawbone	Nike	BASIS
Usable offline without uploading data to server	✗	✗	✗	✗
Makes no commercial use of user data	✗	✓	✓	✗
User retains control of, and rights to their own data	✗	✓	✓	✗
Notifies users of any privacy policy changes	✗	✗	✗	✗
Offers EU-US Safe Harbor protection	✓	✗	✓	✗
Will not gather information about user from other sources	✓	✗	✗	✓
Policy allows for staff to view user data	✗	✗	✗	✓
Doesn't prohibit incomplete or pseudo-anonymous registration data	✗	✓	✓	✗
No provision for logging of user GPS location	✗	✗	✗	✓
Permits complete data removal	✗	✗	✓	✗
States encryption is used to protect user data	✓	✗	✓	✗*
Overall Privacy Score (/11)	3	3	6	3

* As discussed in section 2.4, while BASIS state in their terms and conditions that they encrypt all user information and keep it confidential, they also state in their privacy policy that their databases are not encrypted.

ply with the EU-US Safe Harbor data protection procedures, meaning users may have very few of their regular EU rights with regard to controlling the use and sharing of their own data. While services stated they would anonymise data before selling it or otherwise passing it to other companies, we have identified research indicating that the process of re-identification of such data is becoming increasingly possible. As such, users could potentially face re-identification in the future, based upon their anonymised data, if it was ever compromised or released in anonymised form by the service provider.

Finally, as a result of the analysis of the privacy policies of the services investigated, a hypothetical privacy-preserving health monitoring platform was described and specified, attempting to offer a very high standard of user privacy, and demonstrate that considerable privacy improvements would be possible and practical, to address some of the concerns identified in the policies of existing services.

10. ACKNOWLEDGMENTS

This work was funded by EPSRC Doctoral Training Grant EP/K503174/1, and MaidSafe.net.

11. REFERENCES

[1] A. Act. Health insurance portability and accountability act of 1996. *Public Law*, 104:191, 1996.

[2] BASIS. Basis privacy, November 2012. Retrieved 28 May 2014, http://www.mybasis.com/legal/privacy/.

[3] BASIS. Basis terms of service, November 2012. Retrieved 28 May 2014, http://www.mybasis.com/legal/tos/.

[4] M. Brown. What developers need to know about HIPAA compliance in wearable tech, May 2014. Retrieved 28 May 2014, https://www.truevault.com/blog/what-developers-need-to-know-about-hipaa-compliance-in-wearable-tech.html.

[5] Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel. Unique in the crowd: The privacy bounds of human mobility. *Scientific reports*, 3, 2013.

[6] M. Donner. From the editors: Whose data are these, anyway? *Security & Privacy, IEEE*, 2(3):5–6, 2004.

[7] Fitbit. Website terms and conditions, December 2011. Retrieved 28 May 2014, http://www.fitbit.com/uk/terms.

[8] Fitbit. Privacy policy, January 2014. Retrieved 28 May 2014, http://www.fitbit.com/uk/privacy.

[9] Y. Hong, T. B. Patrick, and R. Gillis. Protection of patient's privacy and data security in e-health services. In *BioMedical Engineering and Informatics, 2008. BMEI 2008. International Conference on*, volume 1, pages 643–647. IEEE, 2008.

[10] P. Jagwani and S. Kaushik. Defending location privacy using zero knowledge proof concept in location based services. In *Mobile Data Management (MDM), 2012 IEEE 13th International Conference on*, pages 368–371. IEEE, 2012.

[11] Jawbone. Privacy, February 2013. Retrieved 28 May 2014, https://jawbone.com/legal/privacy.

[12] M. Kassner. Are you checking privacy policies frequently?, July 2012. Retrieved 28 May 2014, http://www.techrepublic.com/blog/it-security/are-you-checking-privacy-policies-frequently/.

[13] W. J. Long and M. P. Quek. Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise. *Journal of European Public Policy*, 9(3):325–344, 2002.

[14] Nike. EU/UK Nike mobile privacy policy, February 2012. Retrieved 28 May 2014, https://help-all.nike.com/app/answers/detail/article/mobile-privacy/lang_local/en_emea/a_id/38199.

[15] Nike. Privacy & cookie policy, October 2013. Retrieved 28 May 2014, https://help-en-gb.nike.com/app/answers/detail/article/privacy-policy/a_id/16415/p/3897.

[16] P. Ohm. Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*, 57(6), 2010.

[17] A. Pantelopoulos and N. Bourbakis. A survey on wearable sensor-based systems for health monitoring and prognosis. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 40(1):1–12, Jan 2010.

[18] B. Scott. New technologies potentially raise HIPAA concerns, February 2013. Retrieved 28 May 2014, http://www.rctlj.org/2013/02/new-technologies-potentially-raise-hipaa-concerns.

[19] R. Sheinis. Is HIPAA ready for medical wearable devices?, March 2014. Retrieved 28 May 2014, http://www.martindale.com/health-care-law/article_Hall-Booth-Smith-PC_2104782.htm.

[20] G. Steinke. Data privacy approaches from US and EU perspectives. *Telematics and Informatics*, 19(2):193–200, 2002.

[21] B. Wheeler. Give social networks fake details, advises Whitehall web security official, October 2012. Retrieved 28 May 2014, http://www.bbc.co.uk/news/uk-politics-20082493.

[22] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou. Security and privacy in cloud computing: A survey. In *Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on*, pages 105–112. IEEE, 2010.