

The Wearables Privacy Report

October 2014



Foreword

Too Much Information? Wearables Bring a New World of Data but Risks for Communicators

The internet has disrupted every business model and discipline it ever touched. In the communications field, its primary impact has been to bring down the wall between brands and their audiences, so that rather than regular media being the primary proxy, modern media has fragmented, giving communicators far more options and new opportunities to inform and influence.

Wearable technology is just another wave in the sea of disruption that really began with the arrival of the Web. Yet it is a crucial one to understand, with some important communication considerations, because wearables gather and share some of the most sensitive personal data there is. Devices can monitor and divulge so much about an individual's movements, likes, dislikes and their interactions with brands that they're hugely tempting to incorporate in the communications mix.

And as devices gain greater social media functionality, that becomes something of an inevitability. It's not something that's going away, with new product launches gathering pace and the global sales of wearables estimated to reach around 10 million this year, according to a report from Deloitte Consulting.

With little other data available on the topic yet, Zeno wanted to understand more about the consumer privacy issues that surround the evolution of wearables. We wanted to know how consumers feel about personal privacy and how they would feel if brands started to make more use of that data to plan the way they – and others - tell stories.

We partnered with London's Imperial College Business School, part of the Imperial College of Science, Technology and Medicine, on some pioneering research to understand that. The outcome is not a mass market study or a detailed look at how brands plan to use data from wearables. It is an important early snapshot of the some of the current and likely future concerns that consumers have about wearables and their personal privacy – and equally, what information they feel it is appropriate or even useful to share with the wider world.

In particular, we can see genuine concerns around how data is stored or shared with third parties. The majority of consumers seem more than willing to share personal information with the brands they choose to where there is mutual gain for both parties, but are nervous or see potential frustration in sharing it with third parties who may then bombard their busy lives with unwanted content. That has long been a challenge for brand communications when new techniques become available, but carries special significance in the area of wearables, given the intimate nature of the data. Equally, this data becomes of far greater use to brands when they look for trends or insights across larger groups of people, particularly where they're networked together by a common interest or passion. That can be of mutual benefit too, but in a group context the boundaries of personal and collective privacy also need to be understood carefully.

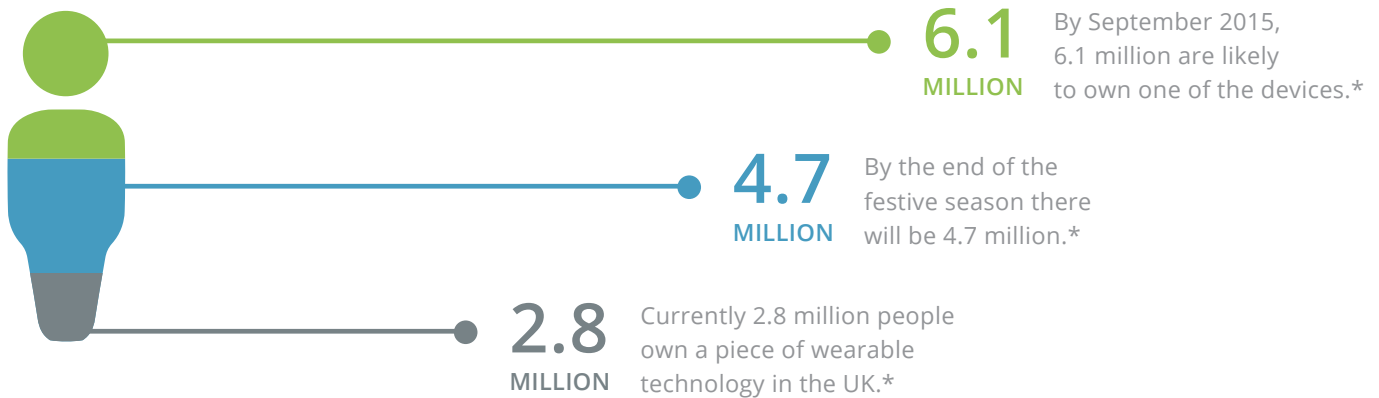
Brands may have more data at their disposal with wearables, but they should also use insight and instinct to better understand their audiences as people, and what their emotional drivers and barriers are. Wearables bring a new layer of data and the communications potential of that information is rapidly becoming clearer.

Wearables: Navigating the Personal Privacy Trade-off



Wearable technology comes in many forms from glasses, watches to bracelets and track and improve consumers' fitness, health and lifestyle.

Wearable Technology ownership:



While it enhances consumer's lifestyle, it raises privacy concerns for customers. The Wearables Privacy Report explores the trade-off between sharing data and privacy fears. It shows:



- **72%** Are aware that information is collected from wearable devices
- **59%** are unaware that information can be shared with third parties
- **55%** do not want their information to be shared with third parties
- **51%** want to know details on how their information will be used
- **MORE THAN 50%** of consumers are willing to share personal information as long as they receive rewards
- **26%** take personal data privacy into account when purchasing a device

TABLE OF CONTENTS

ACKNOWLEDGEMENT	5
EXECUTIVE SUMMARY	6
INTRODUCTION	7
AIMS AND OBJECTIVES	8
SECONDARY RESEARCH	9
PRIMARY RESEARCH	16
PUL FRAMEWORK	22
RECOMMENDATION	26
CONCLUSION	32
REFERENCES	33
APPENDICES	41

ACKNOWLEDGEMENT

First and foremost, we would like to express our appreciation to our clients, Zeno Group for their input into the project. In particular, the constructive feedback provided by Ms. Hannah Williams and Ms. Sasha Manners.

We would like to thank Mr. Maximilian Doelle for all his advice during the planning and development of the research project.

We would also like to express our sincere thanks for the invaluable insights provided by:

Mr. David Keene, Head of Marketing at Google (Northern Europe)

Mr. Bandar Antabi, Vice President of Global Sales at Jawbone

Mr. Gilbert Réveillon, International Managing Director at CityZen Group

We would also like to thank, Mrs. Angela Dalrymple (Program Director MSc Strategic Marketing at Imperial College London) for her advice and assistance during this research project.

Lastly, we would like to express our profound gratitude to Mr. Khalid Alkaf, CEO and Managing Director of Mobily for his guidance and mentorship.

EXECUTIVE SUMMARY

Wearable devices present a prime opportunity for self-quantification and have experienced remarkable growth over the past two years. However, the range of data collected raises concerns among consumers over their privacy and the protection of private information. This concern creates a gap in the market between the trade-off of private information and the utility received by the customer.

The research outlined in this report aims to understand the value consumers place on their privacy and the extent to which they are willing to surrender private information in exchange for utility. Secondly, a range of criteria will be developed for the purpose of assessing the extent to which companies value the privacy of their consumers and the utility which they deliver. A framework will be developed which addresses the gap through improving customer relationships using multiple dimensions (privacy, security and value creation).

Quantitative research was conducted through structured questionnaires which were distributed online to consumers via non-probability sampling. Responses were analysed using SPSS cluster analysis. Semi-structured face-to-face, telephone and email interviews were conducted with Google, Jawbone and CityZen Sciences to apply the grading framework.

Four distinct segments emerged from primary data (Skeptics, Rationals, Curious, Performers), with varying prioritisation in the exchange of privacy and utility. Value derived from utility tends to outweigh privacy concerns for the majority of consumers, especially at the point of purchase.

Zeno Group can utilise the PUL framework to develop guidance for clients regarding customer acquisition, building transparency, developing trust and formulating effective communications.

INTRODUCTION

Wearable devices are small electronic devices which are worn by users. They come in many forms including glasses, watches and bracelets (Chatterjee & Danylyszyn, 2014). In 2012, the global number of wearable smart devices was 8.3 million and expected to grow to 64 million by 2017 (Adams et al, 2014). Smart glasses, fitness bands and watches are predicted to reach sales of 10 million units generating \$3 billion in revenue in 2014 (Lee, Stewart & Calugar, 2014). Currently, the primary objective of wearable technology is to track and improve consumers' fitness, health and lifestyle. Furthermore, wearable technology has potential in shaping how companies engage with their customers. The collection and interpretation of data from wearable devices will be central for companies wishing to maximise financial and brand value.

However, wearable technology is a double-edged sword. While it enhances consumers lifestyle, it raises privacy concerns for customers. Privacy is defined as "the right to control the collection and use of information about oneself" (Dinev & Hart, 2004: p.2). Wearable devices collect identity, activity and contextual information, increasing customer concern about the security of their personal data and reasons for collection. Previous research investigates the impact of wearable technology on consumers and organisations. However, the tradeoff between privacy and utility in relation to consumer behaviour has not been fully examined. Assessing and bridging this gap would play a significant role in creating brand stickiness and excelling in the wearable technology sector.

AIMS AND OBJECTIVES

Companies hunger for data along with consumers growing uncertainty over the safety of their personal information creates a gap in the market. This gap adversely impacts the customer-centric mindset and erodes customer-brand relationships. The aim of the project is to provide Zeno Group with a framework that addresses this gap, thereby positioning them as a thought leader in the highly dynamic wearable technology landscape from a communications perspective. To this purpose, a platform will be created through which privacy, security and value creation can be addressed.

To understand the value that consumers place on privacy and the extent to which they are willing to give it up in exchange for benefits, a survey will be designed and analysed. This will help develop a grading system for privacy and utility for different customer segments.

Furthermore, criteria will be identified using secondary research and interviews to which companies can be assessed based on the value they place on customers' privacy, for example how upfront they are regarding the collection and usage of personal information. Companies will also be graded based on the level of utility they deliver.

The companies scores will be compared with the scores of the different consumer segments identified through primary research. The difference will then be calibrated on a litmus scale that reads red when the gap is significantly large and green when the gap is small. Based on the size of the gap, Zeno Group could provide recommendations on the steps companies should take to acquire the right customers and build behavioural loyalty.

SECONDARY RESEARCH ANALYSIS & FINDINGS

The Changing Face of Privacy

The concept of privacy is continuously evolving as new technologies are introduced. With the digital revolution, rise of social media and diffusion of smartphones, it can be argued that the concept of privacy is losing its meaning.

Typically, users willingly provide personal information, suggesting that people are comfortable with making their data public in order to benefit from a service. However, the general public might not understand that data can be shared between companies and used for purposes which lack an immediate benefit to the consumer. Some users may be alarmed knowing that Twitter sells information (i.e tweets) to social media analytics companies and consumer brands for data mining purposes (Luckerson, 2013). This sparks debates around privacy and gives rise to a need for transparency to establish on-going trust. For privacy debates surrounding Facebook and Apple, refer to Appendix 1.1.

Public Perception

The rapid exchange of information and increased connectivity fuelled by the digital revolution has transformed public perception of private information (Figure 1). Recent discussions highlight a disproportionate relationship where one-way transactions have allowed organisations to collect large amounts of private information with limited gains for the customer. The trend today is towards consumers realising the value of their personal data as an asset. They are learning to make use of this asset in form of exchanges. Consumers are becoming increasingly savvy with their information, as 53% of the UK population recognise the value of using their personal data in transactions (DMA, 2012). Moreover, 90% prefer to have greater control over their personal information and 50% want to know details on how it will be used (DMA, 2012; McCann, 2012).

Thus, consumers are more willing to share information. Consumers seek to build relationships with businesses which can provide clear incentives (DMA, 2012), especially younger age groups (“digital natives”) who grew up in a connected world (McCann, 2014). Hence, consumers are more willing to commit to businesses they can trust. This gap is substantiated by the fact that 60% of consumers do not agree that they receive adequate benefits in exchange for their personal data (DMA, 2012).



Figure 1: Public Perception

Adapted from Accenture (Accenture, 2014)

No Trust, No Relationship

The following infographics (Figure 2 and 3) illustrate how consumers confidence and online trust in the UK is decreasing, with 89% concerned about their online privacy. One of the major causes of concern is that 60% of businesses share their personal information with other companies (Truste, 2014).



Figure 2: (Truste, 2014)

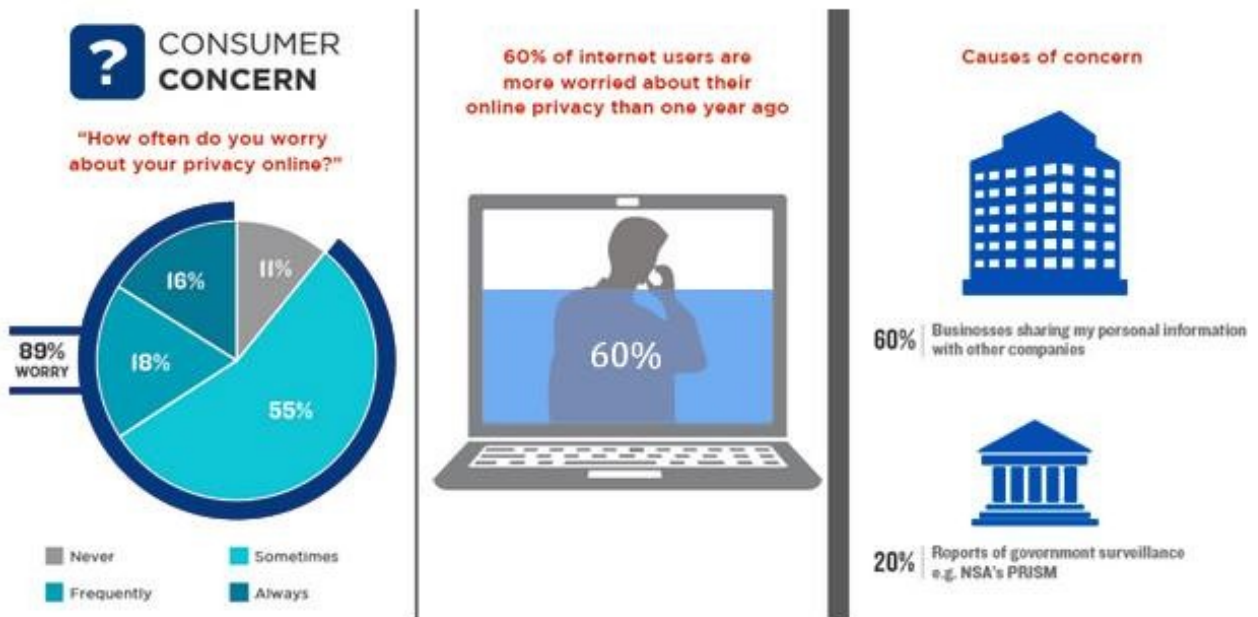


Figure 3: (Truste, 2014)

Privacy concerns reduce consumers trust in brands, affecting the long-term customer-brand relationship (Brown & Muchira, 2004). Research has shown that trust increases loyalty by 22% to 44% (Halliburton & Poenaru, 2010). For instance, Google has maintained its top position amongst the top 20 trusted companies for 7 years (Ponemon Institute, 2013). Consequently, Google has the 11th highest Net Promoter Score (Temkin Group, 2012). However, with the introduction of Glass, Google should be more cautious, as research reveals that 59% of consumers fear their privacy will be eroded by disruptive technologies (Ponemon Institute, 2013). To overcome this, Google should understand that consumers want a two-way relationship, whereby they are willing to give up their private information in exchange for value that enriches their life (Accenture, 2014).

Impact of Privacy Breaches

Disruptive technologies emerge with loopholes putting a massive pool of information at risk. The reported data breaches in the US hit a peak in 2009 with 223,146,989 breaches. However, companies have been observably more cautious in protecting data as the number of US data breaches dipped to 16,167,542 in 2012 (Hess, 2013) (Figure 4). Still, the number of breaches in 2013 is massive and negatively impacting a large consumer base.

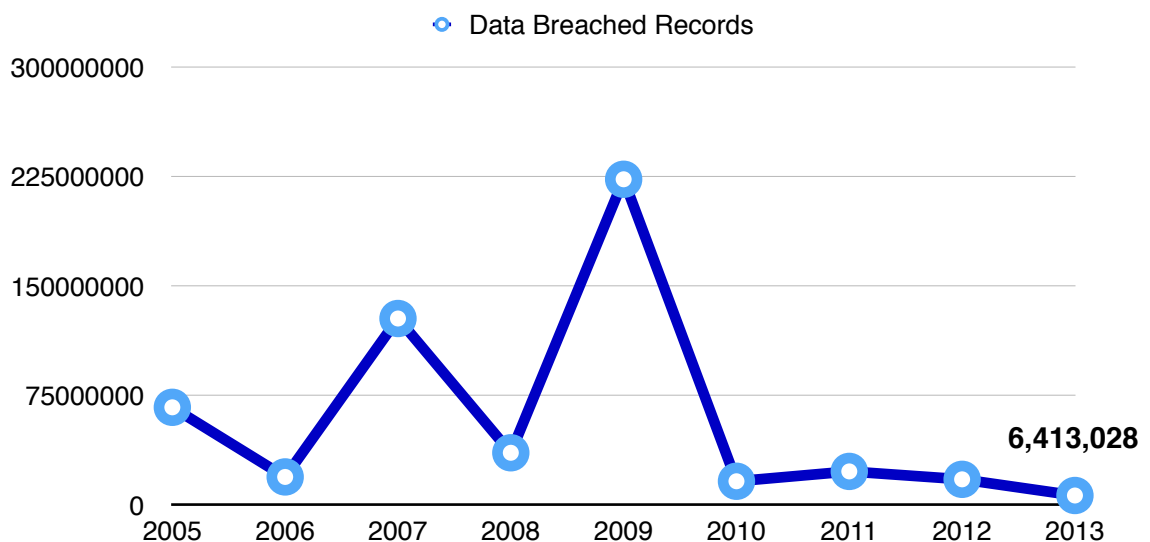


Figure 4: Data Breached Records

Refer to Appendix 1.2 for a timeline of fines from data breaches, types of breaches and potential post-breach damages.

The Pending Regulatory Environment

The recently passed directive on EU privacy law (EU Data Protection Directive 95/46/EC) imposed stricter regulation on liability rules for third party providers, compliance with privacy rules (Curtis, 2014). The implicit consent model was also heavily reformed (Curtis, 2014). The intention to penalise companies upward of 5% of annual global turnover shows that protection of private data will remain a major concern for businesses in the forthcoming period.

The one-stop shop model, using a lead authority to process local complaints is gradually becoming more likely, as the territorial scope of data protection regulation is currently being reformed (Tech Week, 2014). The recent Google case “Right to be Forgotten” created an inflow of 70,000 proposals within the first month, indicating a redistribution of power over private data from a paternalistic approach to an empowered-user approach (FAZ, 2014). Yet, existing loopholes in data protection indicate regulatory reform is likely to continue in light of recent cases. For further details on the challenge of anonymisation and the pending regulatory environment, refer to Appendix 1.3.

The Utility Equation

Wearable devices deliver functional, emotional and augmented benefits that revolutionise consumer lifestyle. Research reveals that consumers are primarily drawn to the functional benefits of wearable technology, particularly amongst early adopters and early majority (Accenture, 2014). A poll of 2,000 UK adults showed that 46% of respondents believe that wearables boost their confidence, strengthen their love life (27%) and make them feel more in control of their lives (53%). Furthermore, 70% of early adopters take an interest in benefits ranging between

physical fitness, sleep quality and navigation (Accenture, 2014). Lastly, 81% of UK respondents claim their personal ability had been enhanced by wearable devices (Brauer and Barth, 2013).

Wearable devices also deliver emotional benefits through marketing them as lifestyle products. They connect to social media and give consumers a sense of community. For example, Google Glass has partnered with Luxottica to improve the design of the product and lower barriers to adoption (Lawler, 2014).

The Long Tail of Wearable Technology

Wearable devices also deliver augmented benefit given that they have a long tail nature (Gownder, Voce & Snow, 2014). Cost-effective modes of reaching niches enables the delivery of contextualised and personalised benefits. A one-to-one customer experience is delivered via Jawbone Up, whereby marketers, using Insight Engine, infuse food consumption, sleep cycle, activity trends and location to recommend the suitable time to drink coffee without affecting sleep cycle. Refer to Appendix 1.4 for previous research on the infinite possibilities presented by wearables.

Privacy Commerce

Everything comes at a cost and the cost of utility is privacy. However, consumers are pragmatic and are willing to trade their personal data for value under certain conditions (Figure 5). More than 50% of consumers are willing to share personal information as long as they receive rewards (Accenture, 2014). This highlights the trade-offs between privacy and utility takes place in the form of negotiation.

Although several researchers touch upon the privacy-utility trade-off, they do not examine whether consumers are willing to give up more privacy for a certain type of benefit over another (Brauer & Bath, 2013; Lawler 2014). Furthermore, the

majority of the research tests privacy and utility in isolation, whereas they should be tested together to understand the true trade-off.

Figure 5: Privacy Commerce



70% are willing to share their personal information for a reward, assuming only their provider uses the data.



65% would share their personal information if the provider abides data protection laws



Only 26% would share their information if their data were provided to a third party

Adapted from Accenture(Accenture, 2014)

PRIMARY RESEARCH METHODOLOGY, ANALYSIS AND FINDINGS

Methodology

From the consumers' perspective, primary research was conducted to understand consumers' attitudes towards data collection from wearable devices. The research aim was to identify overall trends and develop personas based on the respondents' trade-off between privacy and utility. To this purpose, a 17-question survey was created and distributed online through non-probability sampling. Respondents were screened according to familiarity with wearable technology (medium to high familiarity). The questions together with their validation can be found in Appendix 2.1.

The data collected through the 130 responses was analysed with SPSS to identify correlations between variables and recognise distinct segments of customers (Appendix 2.2).

An interview was conducted with Mr. Maximilian Doelle to act as a foundation for determining the privacy and utility components on which manufacturers were graded. Additional face-to-face, telephone and email interviews (Appendix 2.3) were also carried out, in order to apply the framework to Jawbone, CityZen Sciences and Google. Subsequently, the scores were compared with the different customer segments to identify possible gaps and give recommendations.

Analysis & Findings

Digital trust negotiation

Although the majority of respondents (72%) were aware that information is collected from wearable devices, 59% were unaware that information is shared with third parties. Moreover, research revealed that 55% of consumers do not want their

information to be shared with 3rd parties (McCann, 2012). This stresses the importance that companies should put on educating consumers on the process of collecting and sharing information. Although consumers are uncomfortable sharing their personal information, their willingness to share increases when they receive personalised offers. This shows that consumers' privacy concerns diminish as the level of utility rises.

Customers understand that a trade-off exists. Those that do not want to make privacy concessions are insignificant in number and unfamiliar with wearable technology. The research findings show that in general wearable devices are perceived as functional products rather than emotional products. Respondents seek functional health-related benefits like staying fit, which are considered more important than social benefits such as becoming part of a community of users.

The results also reveal that the more expensive the device (Google Glass relative Nike FuelBand), the more personal data people are willing to share. Thus, it can be inferred that people are willing to give more information because they recognise the link to the utility they may obtain and their 'fear of missing out' on benefits is stronger than the costs of the device. Yet, consumers are usually more willing to provide information which is relevant to the service delivered.

The Illusion of Privacy

Purchase determinants include the devices' look and feel, price, and most importantly, the metrics they allow users to measure. Only 26% of respondents take the collection of private information into account when purchasing, which underscores that value outweighs privacy concerns. In general, it can be concluded from the research that, when it comes to wearable technology, privacy concerns are a preconception rather than an actual issue. Furthermore, consumers that were aware of information being collected from wearable devices and shared between

companies prior to completing the survey are less uncomfortable with it compared to consumers that were not previously aware. In other words, it can be said that privacy becomes a greater concern when it is made salient.

These findings are consistent with the Infosecurity Europe study, which showed that 71% of office workers were willing to trade their password for a candy bar (BBC, 2004). Therefore, it can be inferred that privacy is not a concern as long as utility is taken in exchange.

The infographic in Figure 6 summarises the main primary research insights.

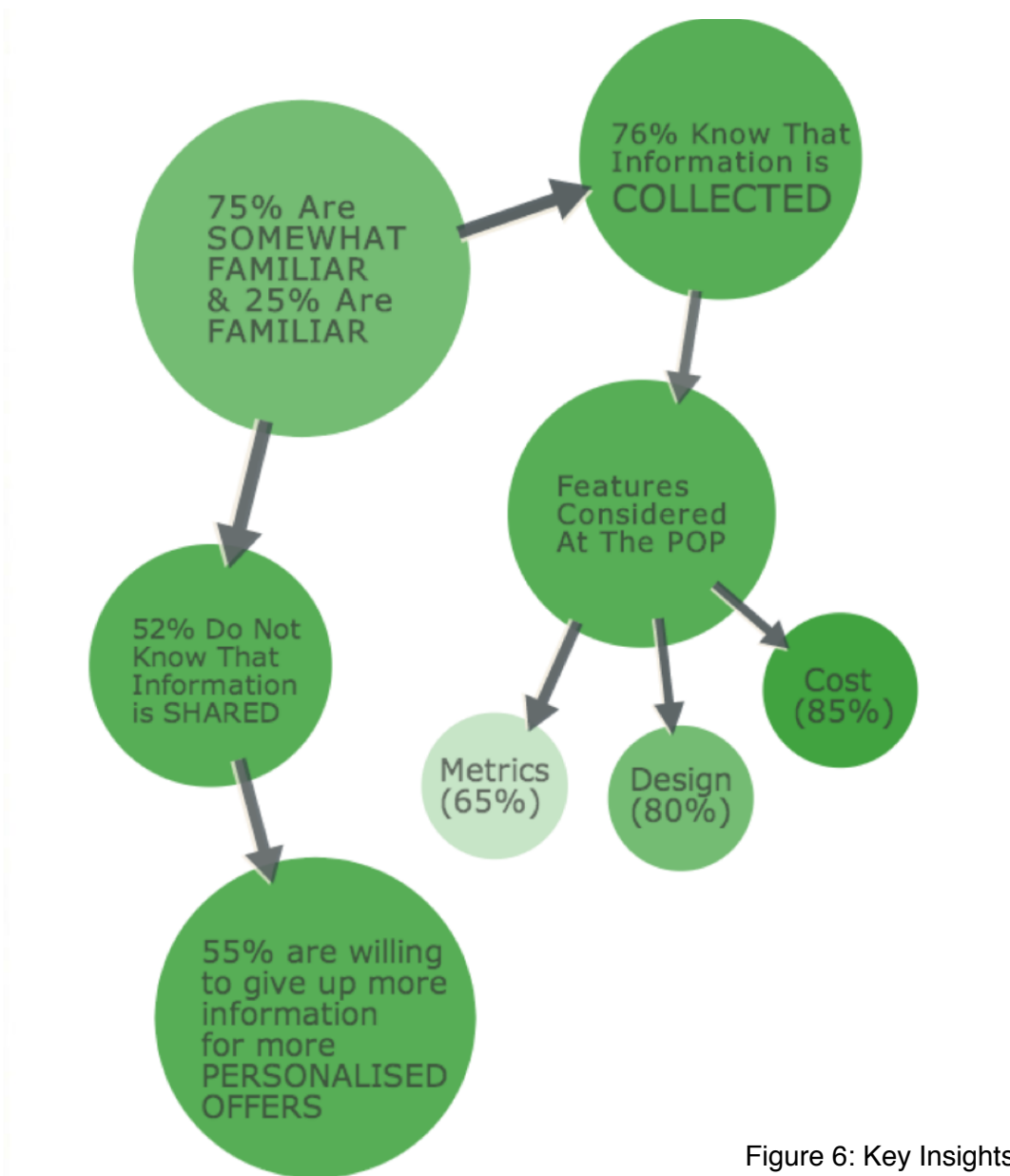
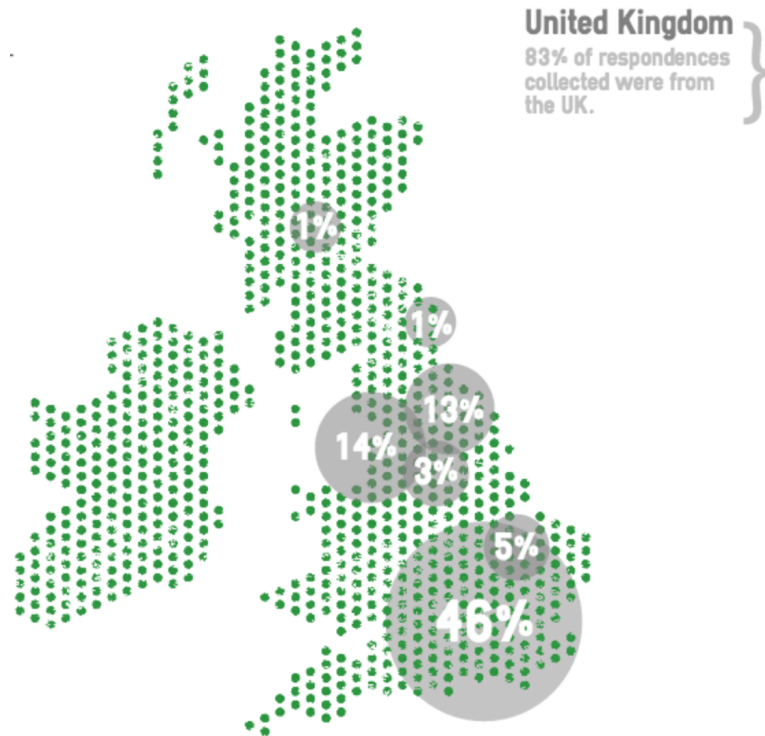


Figure 6: Key Insights

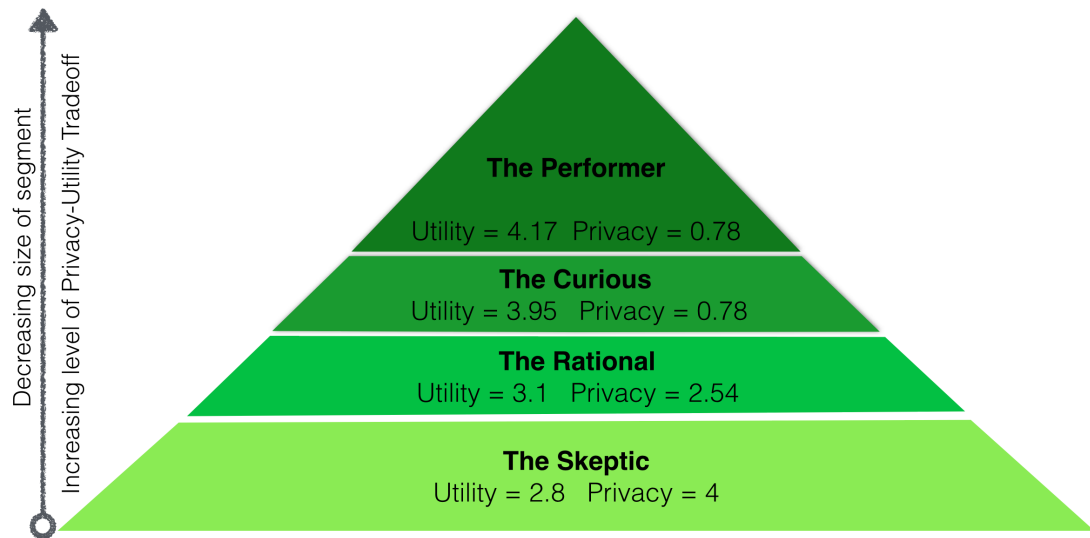
Location of Respondents



Trade-off Personas

The results indicate that different trade-offs exist among consumers. The following profiles were developed, whereby the utility grading represents the consumers perceived attractiveness of device benefits and the privacy grading represents the importance consumers place on safeguarding their personal information. When relevant, information from secondary research was matched to the different personas to make the profiles more comprehensive (Appendix 2.4). The personas are visually represented in Figure 7.

Figure 7: Tradeoff Hierarchy



The Skeptic

This group is skeptical about the benefits of wearable devices. While they are aware that such devices may lead to a healthier lifestyle, they are laggards in their adoption. They are price sensitive. The majority are baby boomers belonging to the digital migrants population, which grew up without Internet connectivity. This segment has a utility grade of 2.8 and a privacy grade 4.

The Rational

They are willing to provide fitness, food and health information in return for functional benefits. They are logical and look for practical products. They have an understanding of technology and how personal information can be used (Brauer and Barth, 2013). In fact, they are not willing to provide identity and location because they know that the product can function without such information. They are not as comfortable in giving up information for social and augmented value. The Rationals value the devices' look and feel as much as the metrics it measures, which reflects their appreciation for all things practical. No clear demographic profile emerged from the findings, as this particular profile emerged across multiple age groups (18-25,

26-35, 36-45, 46-55). This segment has a utility grade of 3.1 and a privacy grade of 2.54.

The Curious

They are comfortable sharing all types of information in exchange for functional and social value. They enjoy challenging others and are intrigued by all things new. They find structures and rules limiting and are interested in imaginative solutions, which is reflected by their willingness to share more information to receive augmented value and contextualised offers. This segment has a utility grade of 3.95 and a privacy grade 1.47.

The Performer

They are social, trendy and love having a good time. They buy wearable devices to be part of a community and express their trendy personality. They value their self-image among reference groups and want to be the centre of attention. Besides design and brand name, they also consider the price of the device. The fitness and health value is not a primary motivator for buying the device. They are also willing to give up more personal information for more personalised offers. The majority of respondents that fall in this segments are under 18 years old. This segment has a utility grade of 4.17 and a privacy grade of 0.78. In general, research does not reveal significant differences across geographic location or education.

The Privacy-Utility Litmus

The PUL framework (Figure 8) has been developed to address the privacy-utility gap in the wearable technology space.

Company

Consumer

Company Privacy vs. Utility Scorecard

Factor	Component
Privacy	Quantity
	Transparency
	Confidentiality
	Data Protection
	Salability
Utility	Functional value
	Emotional value
	Augmented value

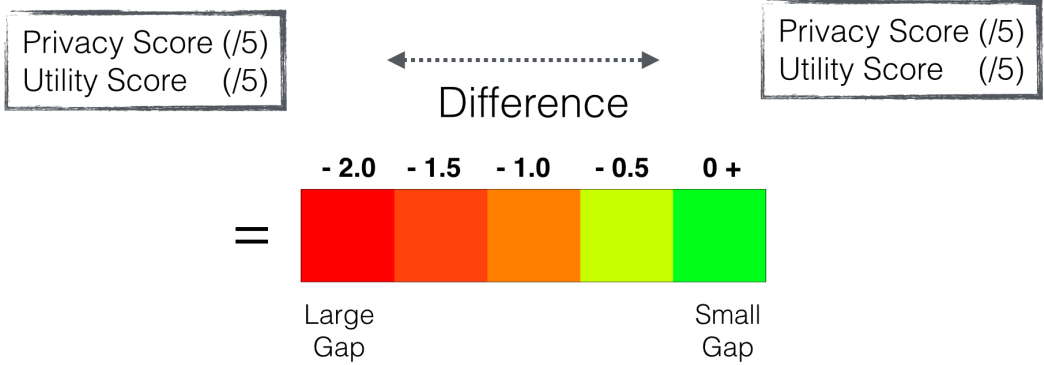
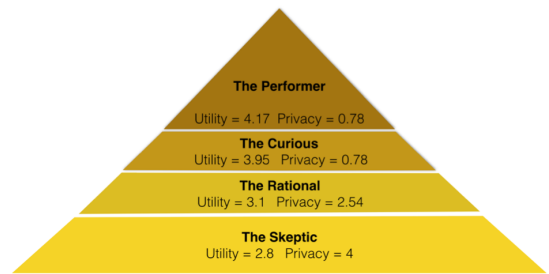


Figure 8: PUL Framework

Based on interviews and secondary research insights, privacy has been broken down into the following sub-components.

- **Quantity:** The amount of data collected and saved from wearable devices, including contact details, fitness and health information, in-app behaviour and location. Companies should not collect information that is not needed to deliver the promised benefits. The amount of information collected is both a risk and an

- opportunity for companies: the higher the quantity of information stored, the greater the cost of breach. Ideally, the information should be adequate, relevant and not excessive (Data Protection Act, 1998).
- **Transparency:** The degree to which a company informs consumers about the information collected and explains the value added to consumers. Privacy policy should be clear and concise to ensure easy consumer reach and education. Transparency is key, as 51% of consumers want to know details on how their information will be used (McCann, 2012).
 - **Confidentiality:** The amount of data that can be disclosed without consumer consent (International Charter, 2011). Information should be used for limited, specifically stated purposes (Data Protection Act, 1998). Privacy policy should include the type of information collected, third parties shared with, reason for sharing and benefits of sharing.
 - **Data protection:** The degree to which information collected is kept safe and secure (Data Protection Act, 1998). There are three components to data protection for wearable devices. First, the security of the operating system used to connect the device to the companion app. Connection and data transfer should be secured through end-to-end encryption of data (Doelle, 2014). Second, the location of data processing. Data processed in the Internet instead of computers faces higher risk of breach because it is easier to access (Doelle, 2014). Third, the storage and aggregation of data. Data that is aggregated has a higher impact if breached as opposed to deleting the data after processing (Doelle, 2014). Companies should also have a secure data protection software (McAfee, 2014).
 - **Salability:** The act of selling the information collected to third parties. Companies need to obtain consent from consumers by clearly outlining their intentions to disclose information to external companies. Grading will not only take into consideration if consent was taken but also the type of information sold.

The above factors will be given a grade out of 5 along with an explanation for the grading (Appendix 3.1). The overall privacy score is an average that assumes that all factors are equally weighted.

The utility delivered by companies will be graded based on the following:

- **Functional Value:** The second layer of the brand dimensions of differentiation (Merlo, 2013). It includes: fitness tracking, sleep cycle, food consumption pattern, alarms, water resistance, comfortability, durability, compatibility with other devices, design and tag price of the wearable device relative to competition (Wellocracy, n.d.). Glasses benefits includes easy navigation, web search and hand-free connection to others (Keene, 2014).
- **Emotional Value:** Derived from the brand image and communication messages. It includes: feeling trendy, active or health-conscious, being part of a community and consistency of brand personality (Antabi, 2014).
- **Augmented Value:** The third layer of the brand dimensions of differentiation, which entails delivering unexpected value that differentiates a company in the market (Merlo, 2013). It includes the apps the device can be connected to, real-time messages, customer service and guarantee. It also include using perceptive design to deliver targeted and real-time communications (Essence, 2014).

The above factors will be given a grade out of 5 along with an explanation for the grading. The overall utility score will be an average which assumes that all factors are equally weighted. Refer to Appendix 3.2 for grading system details.

A company's scores are compared with the target market's (trade-off personas) privacy and utility scores to derive the size of the gap and provide a value proposition for each respective market. A gap exists when the difference between the company grading and the consumer grading is negative and a gap does not exist when the difference is zero and above (Figure 9). For example, a company that has -1.2 privacy gap shows that consumers value privacy more than the company and a company with a +1.2 utility gap shows that the company puts more value on

utility than consumers. Zeno Group can accordingly advise clients that aim to acquire new customers on the ideal target market(s) and develop respective communication strategies. On the other hand, Zeno Group can advise clients that aim to build sustainable loyalty with their existing consumers on tactics that best appeal to each segment. For companies that cannot determine which segment they are targeting, Zeno Group can run the survey provided in Appendix 3.2 to determine the segment classification.

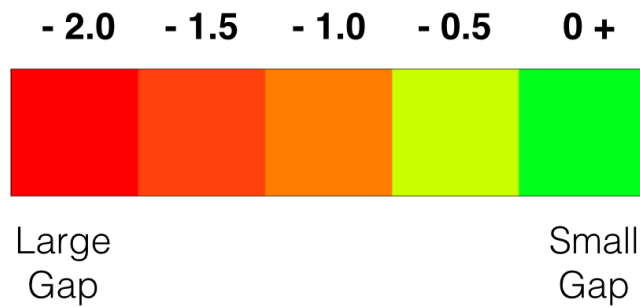


Figure 9: Litmus



Figure 10: GAP Analysis

RECOMMENDATIONS

The recommendations are based on steps Zeno Group should consider to bridge the gap between the company and consumer through addressing the privacy-utility trade-off.

Narrowing A Gap

“A large gap can arise from a lack of transparency or a shortfall in utility”

1. The Forefront of Transparency: The transaction of customer data will require companies to build relationships based on trust. The consensus among customers that data can be used as an asset means consumers must be able to feel more in control over their data. Building a solid foundation on trust can thus only be achieved by empowering the customer base with control over the data exchange process. The basis for building trust can be achieved by being more transparent with private information.

Three Levels of Transparency: Companies can follow a set of guiding principles for building transparency with their customer base

Level	Activity
1. Basic	Allowing customers to view, modify and delete personal information collected by the organisation
2. Sophisticated	Providing clear interfaces of their individual customer profile with purchase history, recommendations and interests; allows customers to control information and gives greater incentive to improve the accuracy of their own profile
3. Advanced	Provide access to personal data with analysis tools to monitor information and discover patterns in their own purchase history (form of public records system) (Galgey, 2012)

A. Empowering the customer - Instead of only providing lengthy privacy policies, companies should provide a summary with a clear explanation of the type of data collected and the benefit to the customer. Giving the customer greater control over this process builds trust and provides an incentive to share personal data.

B. Reciprocity - Since customers are becoming more savvy there needs to be a clear focus on benefits. The reasons for opting-in to services need to be framed accordingly with a focus on both functional and emotional benefits. Companies that share information with third parties need to prove how opting-in to this model can enrich the users experience. Communications need to be tailored according to each user profile to provide a compelling incentive.

2. Customer Acquisition Profile: When the gap emerges from a utility inferiority, companies need to adjust their value proposition to improve their communication strategy (Figure 11). Using the interview with the International Managing Director of CityZen Sciences, and Marketing Manager of Google , David Keene, two case application were developed to serve as an example for a new companies that face a gap in the wearable technology market (Appendix 4.1). The case and the recommendations provided serve as a guideline on how Zeno Group could implement the framework for its clients.

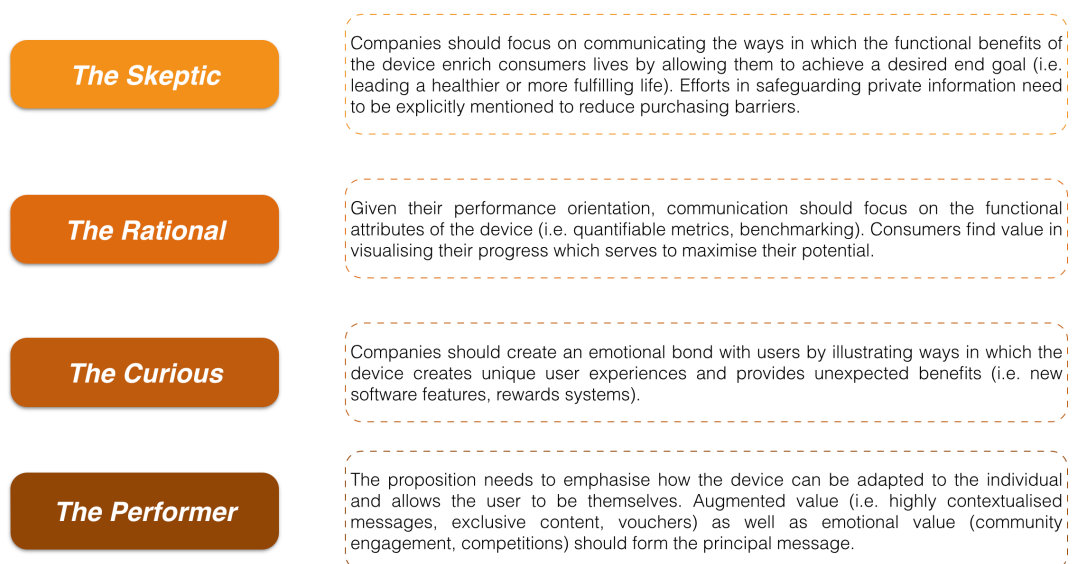


Figure 11: Value Propositions

Digital Trust Leadership

After bridging the gap companies should strive to maintain leadership in the wearable technology space.

1. Big Data + Cognitive Analytics = Contextual Insights

A satisfied customer is not necessarily a loyal customer. To win loyalty, companies should deliver unanticipated value that delight consumers. Today, big data together with Cognitive Analytics can be used to engage and retain consumers. Cognitive Analytics is a technique that uses sophisticated software to run queries on information from various sources and develops actionable insights for real-time decision-making. It acts as a layer on top of traditional analytics to increase speed and accuracy. Cognitive analytics processes massive information to understand relationships using influence and causality, operating like a human brain that continuously improves its insights without human intervention (Chatterjee & Danylyszyn, 2014). Companies such as Jawbone, which aggregate data could implement cognitive analytics to predict the best meal for consumers using food consumption history, previous preferences, location and impact of certain nutrition on health and fitness goals. Delivering such context-rich personalisation that is relevant and unanticipated delights consumers and taps into behavioural loyalty (Merlo, 2014).

2. Think Like Consumers

Another way to delight consumers is to reposition the business to deliver solutions as opposed to products. Existing manufacturers should shift the focus from listing features and sensor capabilities to the ways wearable devices enrich consumers' lives (Eisingerich, 2014). The communication strategy should portray why consumers should buy a device because consumers do not buy what companies do, they buy why they do it. For example, Google Glass is not about navigation, search engine or taking pictures; it is about creating a frictionless

technology that gives consumers universal accessibility while being hands-free. Through this message, Google communicates that it values consumers need for less intrusive technology and more human interactions. Thus, building a communication strategy based on mutual values and focusing on end-goal benefits creates customer-brand attachment and enables sustainable attitudinal and behavioural loyalty.

3. Educate, Educate, Educate

Contextualised information delivers sustainable engagement, yet it raises further privacy concerns on how much companies know. To respond to this challenge, companies need to educate consumers on the added value from information collection. The three cases analysed (Appendix 4.1 and 4.2) showed that companies have clear privacy policy yet they fail to clearly outline their utility to consumers. By dedicating a section for the value added to consumers, trust in brands will improve and so will the relationship. Secondary and primary research suggest that consumers are willing to give up privacy for utility; therefore, companies should not be concerned about consumers' negative reactions because consumers appreciate companies' efforts in being upfront and honest.

Using the Interview with the Vice President of Global Sales at Jawbone, a case application was developed to serve as an example of a company in a leadership position. The case and the recommendations provided serve as a guideline on how Zeno Group could implement the framework for its clients (Appendix 4.2).

Crisis Response Management

Companies should build a culture of consumer trust, data control, employee commitment and crisis team agility. The key target of managing a data breach is to minimise the cost and the time it takes to recover to preserve the brand image and the trust of consumers (George, 2014). To control damage when dealing with a

privacy breach, companies should follow a predefined escalation policy consisting of the steps that should be taken when crisis erupts (Rowles, 2014). Companies should also dedicate a crisis response team with interdepartmental skills to handle and analyse the situation. Combining these elements with automated response management tool could further optimise the management of a privacy breach (George, 2014). Proactively informing customers about the degree of impact and the steps taken to reduce the damage to personal information preserves company's value proposition and consumers' trust.

RECOMMENDATIONS

Technology advancements coexist with privacy issues. Consumers tend to be uncomfortable about their personal data being collected and shared. Nevertheless, when it comes to buying a wearable device, privacy does not play a major role in the purchase decision compared to other determinants such as price or design. This clearly shows that a trade-off exists between privacy and utility.

The PUL framework addresses this trade-off and aims at providing a tool for organisations to assess themselves and their customers based on the value placed on privacy and on the benefits offered (by the company) and sought (by the consumer). Recommendations are provided as to what measures to put in place when the framework reveals a gap.

The suggested framework addresses the project brief submitted by Zeno Group, in that it helps to understand the role that privacy plays in the marketing strategies of wearable devices' manufacturers. The extensive underlying research provides Zeno Group with a knowledge base that is useful for them to meaningfully engage with organisations in the wearable computing space. Finally, the case applications represent an example of recommendations that Zeno Group could give as a communications agency.

Given the dynamism of the wearable technology industry, the PUL framework is envisioned as a ready-to-use tool as well as a thought process. In this sense, it can be adjusted and updated whenever significant advancements in the wearable computing space occur.

Conclusion

Excitement, Nerves and Handle with Care

The Wearables Report is a brief but, we feel, important early look at the issues, attitudes and concerns consumers have about their use of wearable technology in the UK and how it can enable them to forge even closer relationships with brands. The data gathered is qualitative, but through partnership with Imperial Business School we have been able to gain a closer understanding of what the communications considerations are today, and how they are likely to develop.

Drawing definitive conclusions from a relatively short exercise has its limitations of course. We believe that the research gives us clear indicators and a number of useful insights however. Above all, we see three primary issues emerging from it:

1. Greater intimacy, greater expectations: ownership of data and transparency about how it may be used by brands or shared with third parties is the biggest single communications issue for brands around wearables. Wearables are giving rise to a more intimate relationship platform between people and brands of all kinds. While these are still relatively early days, more intimate communication enabled by media worn on the body brings with it fundamental requirements for a heightened level of trust. Greater intimacy brings greater expectations, and consumers who trust brands with data expect brands to treat this data with care. This also forces a greater need to communicate with individuals on a human level. In exchange for being 'let in' to people's daily lives, brands will need to do more in exchange by communicating more personally.

2. Listening must be mutual: many people are already prepared to give up their personal data to brands via social media. Consumers giving up more and more personal data are going to expect brands to give up more about themselves in return. If brands get that wrong, if they are not prepared to listen and make clumsy attempts to communicate and engage, there is a very real prospect of a backlash. While there may be a big difference in data-gathering functionality between a simple wristband to track fitness and eyewear that can track everything someone sees, technological evolution is likely to give greater capability but brands must understand the role they must play in using them for communication.

3. Power to the network: brands also need to look beyond individuals to the network effect of online communities - powered by wearables. Networks are where influence can really be gained, but also where the stakes are higher. A mistake with one consumer might be forgiven, but crass targeting of large groups with communication around interests or passions will not only leave brands looking out of touch or irrelevant, but can prompt consumers to disengage. Using the knowledge that the data provides responsibly and appropriately, in a perpetual state of learning, is key. Clever communication means understanding that wearables give rise to a privileged, data-driven relationship so brands must gain genuine intelligence, and use it wisely.

If you would like any further information, please do not hesitate to contact us –

Gurjit Hothi

gurjit.hothi@zenogroup.com

+44 (0)20 3047 2072 (D)

+44 (0)20 3047 2400 (O)

@zenogrouplondon

REFERENCES

Abbruzzese, J. (2014) Facebook feels bad that emotions experiment was 'poorly communicated'. Mashable. [Online] Available from: <http://mashable.com/2014/07/02/facebook-sandberg-emotions-experiment/> [Accessed: 4th July 2014].

Accenture. (2014) "Racing Toward a Complete Digital Lifestyle: Digital Consumers Crave More". Accenture. [Online] Available from: <http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Digital-Consumer-Tech-Survey-2014.pdf> [Accessed 4 July 2014].

Acquisti, A., Friedman, A. & Telang, R. (2006) Is there a cost to privacy breaches? An event study. [Online] Heinz College Carnegie Mellon University. Available from: <http://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf> [Accessed 10 July 2014].

Adams, N., Chandler, J., Messere, B. & Williams-Brown, C., 2014. 14 Digital Trends for 2014 + associated opportunities for brands, London, United Kingdom: Mindshare.

Afroz, S., Islam, A. C., Santell, J., Chapin, A. & Greenstadt R. (2013) How Privacy Flaws Affect Consumer Perception. STAST. [Online] 10-17. Available from: <http://www.eecs.berkeley.edu/~sa499/papers/stast-privacy.pdf> [Accessed 9 July 2014].

American Banker. (2014) "JPMorgan replaces 2M bank cards after Target breach, US". American Banker. [Online] Available from: <http://www.americanbanker.com/syndication/jpmorgan-replaces-2-million-bank-cards-after-target-breach-1064895-1.html> [Accessed 22 July 2014]

Antabi, B. (2014) Jawbone Up Utility and Data Privacy. Interviewed by Alanoud Alkaf, Dev Doowa and Magnus Eldevik [Face-to-Face] 10th July 2014, 11:00.

BBC. (2004) Passwords revealed by sweet deal. [Online] BBC News. Available from: <http://news.bbc.co.uk/2/hi/technology/3639679.stm> [Accessed 23 July 2014].

Betancourt, L. (2014) How companies are using your social media data. Mashable. [Online] Available from: <http://mashable.com/2010/03/02/data-mining-social-media/> [Accessed: 4th July 2014].

Bosomworth, D. (2012) "The Content Marketing Matrix". [Online] Available from: <http://www.smartinsights.com/content-management/content-marketing-strategy/the-content-marketing-matrix-new-infographic/> [Accessed July 21, 2014].

Bothun et. al, (2014) "Consumer privacy: What are consumers willing to share?". PriceWaterhouseCoopers. [Online] Available at: <http://www.pwc.com/us/en/industry/entertainment-media/publications/consumer-intelligence-series/consumer-privacy.jhtml> [Accessed 21 July 2014].

Brauer, C. & Barth, J. (2013) "The Human Cloud: Wearable Technology from Novelty to Production". Rackspace. [Online] Available from: http://www.rackspace.co.uk/sites/default/files/whitepapers/The_Human_Cloud_-_June_2013.pdf [Accessed July 3 2014].

Broersma, M. (2014) "EU To Tighten Data Protection Controls On US Internet Giants". Tech Week Europe. [Online] Available at: <http://www.techweekeurope.co.uk/news/eu-tighten-data-protection-controls-us-internet-giants-146938> [Accessed 21 July 2014].

Brown, M., Muchira, R. (2004) Investigating The Relationship Between Internet Privacy Concerns and Online Purchase Behaviour. Journal of Electronic Commerce

Research [Online]. Available from: <http://www.csulb.edu/web/journals/jecr/issues/20041/Paper6.pdf> [Accessed 17th July 2014].

Budras, C. (2014) "Kampfansage an die Pressefreiheit". Frankfurter Allgemeine Zeitung. [Online]. Available from: <http://www.faz.net/aktuell/wirtschaft/wirtschaftspolitik/google-recht-auf-vergessenwerden-kampfansage-an-die-pressefreiheit-13030042.html> [Accessed 21 July 2014].

Chatterjee, A. & Danylyszyn, A. (2014) "Tech Trends 2014". Deloitte University Press. [Online] Available from: http://www.deloitte.com/assets/Dcom-Luxembourg/Local%20Assets/Documents/Whitepapers/2014/dtt_en_wp_techtrends_10022014.pdf [Accessed 4 July 2014].

Chemi, E. (2014) Investors couldn't care less about data breaches. Business Week. [Online] Available from: <http://www.businessweek.com/articles/2014-05-23/why-investors-just-dont-care-about-data-breaches> [Accessed 8 July 2014].

Combemale, C. (2014) "Data privacy: What the consumer really thinks". DMA. [Online] Available from: http://dma.org.uk/sites/default/files/toolkit_files/data_privacy_-_what_the_consumer_really_thinks_2012.pdf [Accessed 21 July 2014].

Curtis, J. (2014) 5 Ways the new EU Data Protection Regulations will Affect your Business. Computer Business Review. [Online] Available from: <http://www.cbronline.com/news/security/5-ways-the-new-eu-data-protection-regulations-will-affect-your-business-4260066> [Accessed: 4th June 2014].

Daileda, C. (2014) Anger builds over Facebook emotion manipulation study. Mashable. [Online] Available from: <http://mashable.com/2014/06/29/anger-facebook-emotion-manipulation-study/> [Accessed: 4th July 2014].

Data Protection Act. (1998) A The National Archives. [Online] Available from: <http://www.legislation.gov.uk/ukpga/1998/29/section/2> [Accessed 15th July 2014].

Dinev, T. & Hart, P. (2004) Internet Privacy, Social Awareness, And Internet Technical Literacy – An Exploratory Investigation. 17th Bled eCommerce Conference eGlobal. [Online] 2 Available from: [https://domino.fov.uni-mb.si/proceedings.nsf/0/affeedb48669326dc1256ee000317a2b/\\$file/42dinev.pdf](https://domino.fov.uni-mb.si/proceedings.nsf/0/affeedb48669326dc1256ee000317a2b/$file/42dinev.pdf) [Accessed: 23rd July 2014].

Doelle, M. (2014) Wearable Technology Challenges and Opportunities. Interviewed by Alanoud Alkaf and Dev Doowa [Face-to-Face] 7th July 2014, 13:00.

Eisingerich, A. (2014) Lecture 5 “What is the ultimate relationship destination and how does business get there?” [Academic Lecture] (Personal Communication, 10th March 2014).

Galgey, W. (2012) “Privacy - From Data to People”. The Futures Company. [Online] Available from: <http://thefuturescompany.com/free-thinking/privacy/> [Accessed 21 July 2014].

George, T. (2014) When Data breaches boost share prices. eSecurity Planet. [Online] Available from: <http://www.esecurityplanet.com/network-security/when-data-breaches-boost-share-prices.html> [Accessed 8 July 2014].

Gownder, J.P., Voce, C. & Snow, S. (2014) Quick Take: Google’s Smart Contact Lens Project. Forrester Research [Online]. Available from: <http://www.forrester.com/Quick+Take+Googles+Smart+Contact+Lens+Project/fulltext/-/E-RES112721> (Zeno Group). [Accessed 15th July 2014].

Granstra C. & Zbikowski, K. (2014) "Eighty Percent of Consumers Believe Total Data Privacy No Longer Exists". Accenture. [Online] Available from: <http://newsroom.accenture.com/news/eighty-percent-of-consumers-believe-total-data-privacy-no-longer-exists-accenture-survey-finds.htm> [Accessed 21 July 2014].

Halliburton, C., Poenaru, A. (2010) The Role of Trust in Consumer Relationships. ESCP Europe. [Online] Available from: <http://www.slideshare.net/pitneybowes/the-role-of-trust-in-consumer-relationships-pitney-bowes-white-paper> [Accessed: 17th July 2014].

Hess, K. (2013) "Reported data breached records in US from 2005 to present exceed 500 million". ZD Net. [Online] Available from: <http://www.zdnet.com/reported-data-breached-records-in-us-from-2005-to-present-exceed-500-million-7000018991/> [Accessed 5 June 2014].

Holdren et. al., (2014) "Big Data and Privacy: A Technological Perspective". President's Council of Advisors on Science and Technology. [Online] Available from: http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf [Accessed 21 July 2014].

International Charter. (2011) "Confidentiality Policy". International Charter. [Online] Available from: <http://www.internationalcharter.org/confidentiality.html> [Accessed 22 July 2014].

Keene, D. (2014) Google Glass. Interviewed by Alanoud Alkaf, Margherita Capitanio, Dev Doowa and Magnus Eldevik [Face-to-Face] 17th July 2014, 10:30.

Lawler, R. (2014) Ray-Ban and Oakley are working with Google Glass. engadget. [Online] Available from: <http://www.engadget.com/2014/03/24/google-glass-ray-ban-oakley-luxottica/> [Accessed: 10th July 2014].

Lee, P., Stewart, D. & Calugar, C. (2014) "Technology, Media & Telecommunications Predictions 2014". Deloitte. [Online] Available from: <http://www.deloitte.co.uk/tmtpredictions/assets/downloads/Deloitte-TMT-Predictions-2014.pdf> [Accessed 4 July 2014].

Luckerson, V. (2014) Twitter Is Selling Access To Your Tweets For Millions. Time [Online] Available from: <http://business.time.com/2013/10/08/twitter-is-selling-access-to-your-tweets-for-millions/> [Accessed: 4th July 2014].

McAfee. (2014) Business Home. McAfee [Online]. Available from: <http://www.mcafee.com/us/business-home.aspx?CID=MFEen-usMHP002> [Accessed 10th July 2014].

McCANN. (2012) The Truth About Privacy. McCANN [Online]. Available from: http://mccann.com/wp-content/uploads/2012/06/McCann_Truth_about_Privacy.pdf [Accessed 13th July 2014].

Merlo, O. (2013) Lecture 1 Brand Management. [Academic Lecture] (Personal Communication, 7th October 2013).

Merlo, O. (2014) Lecture 5 Managing Customer Relationships Strategically. [Academic Lecture] (Personal Communication, 7th March 2014).

Pace. (2014) Brands, Content Marketers Explore Advertising Through Wearable Technology. Pace [Online]. Available from: <http://www.paceco.com/brands-content-marketers-explore-advertising-wearable-technology/> [Accessed 4th July 2014].

Polonetsky, J. & Tene, O. (2013) "Privacy and Big Data: Making Ends Meet". Stanford Law School. [Online]. Available from: <http://www.futureofprivacy.org/big-data-privacy-workshop-paper-collection/> [Accessed 21 July 2014].

Ponemon Institute. (2011) "2011 Cost of Data Breach Study: United Kingdom". Ponemon Institute LLC. [Online] Available from: http://www.ponemon.org/local/upload/file/2011_UK_COdB_FINAL_5.pdf [Accessed 21 July 2014].

Ponemon Institute. (2013) Ponemon Report- The Post Breach Boom 2013. [Online] Available from: <http://img.en25.com/Web/BlueCoat/Ponemon%20Report-Post%20Breach%20Boom%202013.pdf> [Accessed 6 June 2014].

Ponemon Institute. (2013) 2012 Most Trusted Companies for Privacy. Ponemon Institute [Online] Available from: <http://www.ponemon.org/local/upload/file/2012%20MTC%20Report%20FINAL.pdf> [Accessed: 10th July 2014].

Ponemon Institute. (2014) "2014 Cost of Data Breach Study: Global Analysis". Ponemon Institute LLC. [Online] Available from: <http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=SEL03027USEN> [Accessed 21 July 2014].

Reveillon, G. (2014) D-Shirt Utility and Data Protection Challenges. Interviewed by Alanoud Alkaf [Email and Telephone] 14th July 2014.

Riley, M. & Lawrence, D. (2014) As data breaches woes continue, Target's CEO resigns. Business Week. [Online] Available from: <http://www.businessweek.com/articles/2014-05-05/as-data-breach-woes-continue-targets-ceo-resigns> [Accessed 10 July 2014].

Rowles, D. (2014) Lecture 5 Social Media Engagement Workshop. [Academic Lecture] (Personal Communication, 5th February 2014).

Segelken, H. R. & Shackford, S. (2014) News feed: 'Emotional contagion' sweeps Facebook. Cornell University. [Online] Available from: <http://news.cornell.edu/stories/2014/06/news-feed-emotional-contagion-sweeps-facebook> [Accessed: 4th July 2014].

Temkin Group. (2012) Net Promoter Score and Market Share For 60 Tech Vendors. [Online] Available from: <http://experiencematters.wordpress.com/2012/05/14/net-promoter-score-and-market-share-for-60-tech-vendors/> [Accessed: 10th July 2014].

Truste. (2014) "Truste Privacy Index 2014 Consumer Confidence Edition". Truste. [Online Image] Available from: <http://www.truste.com/uk-consumer-confidence-index-2014/> [Accessed 5 July 2014].

Violino, B. (2011) How data breaches can affect brand and reputation. CIO Insight. [Online] Available from: <http://www.cioinsight.com/c/a/Security/How-Data-Breaches-Can-Affect-Brand-and-Reputation-888678/> [Accessed 9 July 2014].

Wellocracy. (n.d.) Wearable Activity Devices Comparison Chart. [Online] Available from: <http://www.wellocracy.com/wearable-activity-trackers/wearable-activity-tracker-chart/> [Accessed: 10th July 2014].

Willetts, D. (2014) "2014 Information Security Breaches Survey". PriceWaterhouseCoopers. [Online] Available from: <http://www.pwc.co.uk/audit-assurance/publications/2014-information-security-breaches-survey.jhtml> [Accessed 21 July 2014].

APPENDIX 1.1

Case study 1: Facebook's Emotion Manipulation Study

A study conducted by Facebook and a team of social scientists was released, where users' news feeds were manipulated and the effect on their mood and emotions observed (Cornell University, 2014). Though Facebook's data-use policy informs users that data may be utilised for analysis, the news raised privacy concerns and the ethics of the study was questioned (Daileida, 2014). Criticisms were mainly addressed to the fact that the platform environment was manipulated for research purposes without the users involved having agreed or being aware, which might lead to eroded trust in the social network. Facebook's COO later admitted the experiment was 'poorly communicated' (Abbruzzese, 2014), suggesting that more transparent communications play a crucial role in the use of data by organisations perceived as a privacy violation.

Case study 1: Apple's Upcoming HealthKit

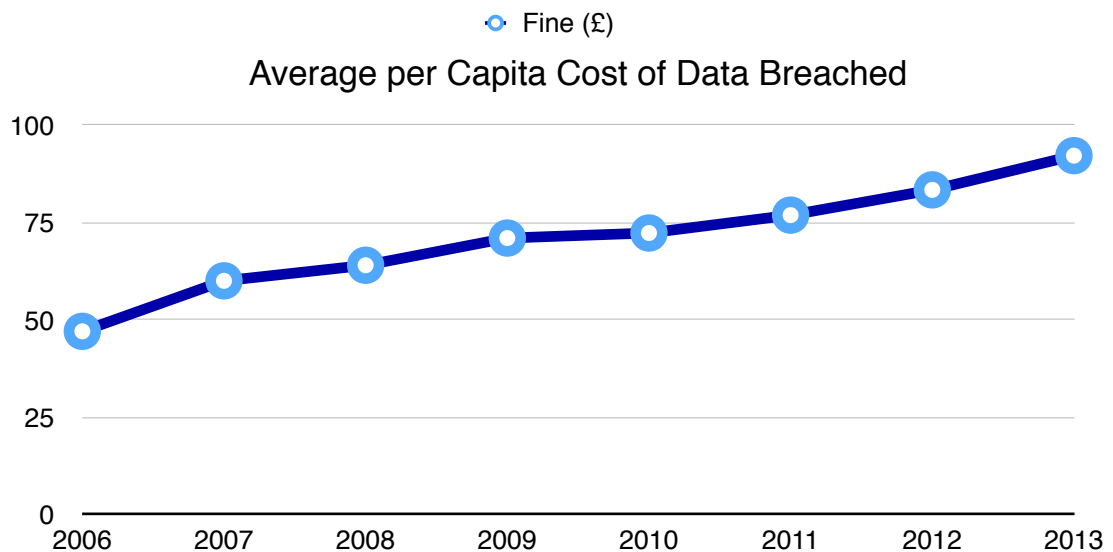
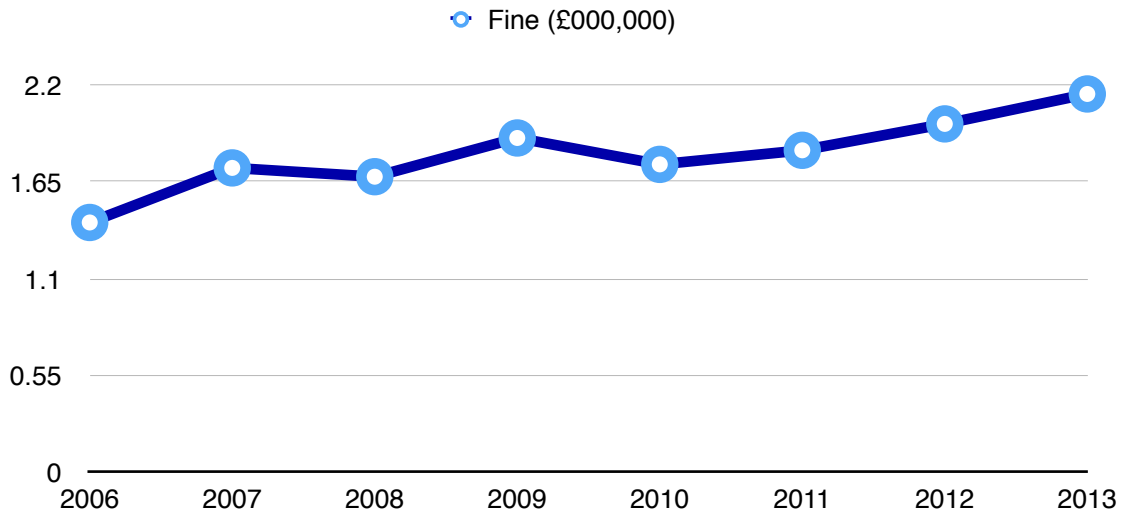
Apple recently announced a Health app, which will be available for iOS 8, alongside a service for developers called HealthKit (Murphy Kelly, 2014). The new application will pull in data from third-party fitness and health-tracking apps, serving as a hub for user's health-related information and contributing to the 'quantified self' (Apple, 2014). Moreover, the data collected could be shared with healthcare providers, turning the iPhone into a 'digital health platform' (Wang, 2014). This news generated privacy concerns, suggesting that Apple will have to focus on security in its communications and provide clear privacy options in order to remove usage barriers.

These cases highlight that technology advancements coexist with privacy concerns. As technology evolves faster than legislation, the debate around privacy will persist with the introduction of future devices.

APPENDIX 1.2

Privacy Breaches Timeline

Regulation has tightened over the past three years, causing a significant rise in fines for privacy breaches across all industry sectors. As regulators impose tougher fines, organisations saw their costs double since 2013. While studies indicate a decline of 7% in business disruption as a result of privacy breaches, a larger number of businesses reported dealing with individual breaches for prolonged periods of time (often exceeding one month)(PWC, 2014).

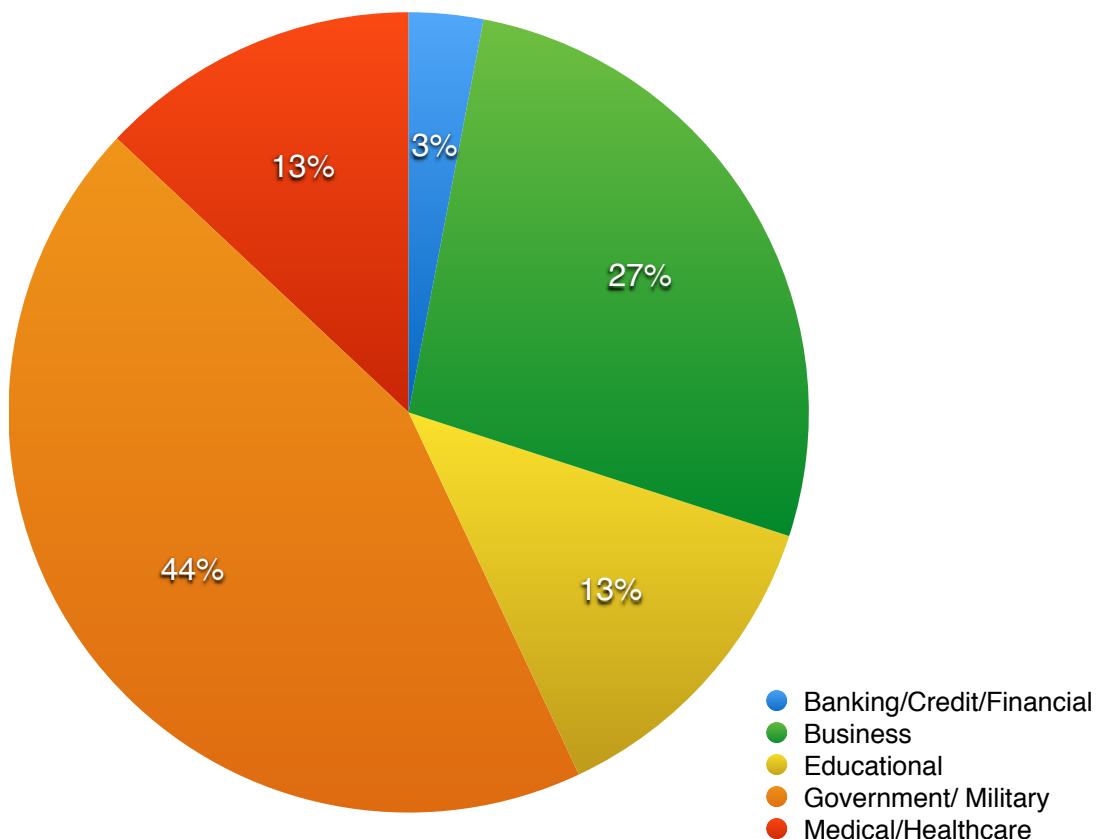


As the new EU Data Protection Directive (Directive 95/46/EC) set in, both small and large organisations were impacted by higher penalties. Small businesses incurred fines ranging between £40,000 to £70,000 marking a sharp rise from £30,000 to £50,000. Large organisations equally saw their costs rise from £1,980,000 to £2,150,000 (Ponemon, 2014). Cost per record breached experienced a historic growth of 10%, reaching an average value of £92.2 (Ponemon, 2014).

Reputational damage has become a major challenge for businesses over the past year, as the wider public has been taking a stronger interest in privacy. Resultantly, individual breaches have received extensive coverage across media outlets fuelling discussions among consumers. While consumers tend to be more forgiving of small businesses (£1,600-£8,000), large organisations faced more intensive scrutiny. Costs incurred as a result of reputational damage rose from £25,000-£115,000 in 2013 to £50,000-£180,000 as of 2014 (Ponemon, 2014).

The 2012 electronic breach statistics break down is illustrated in the figure below.

Electronic Breach Statistics Breakdown

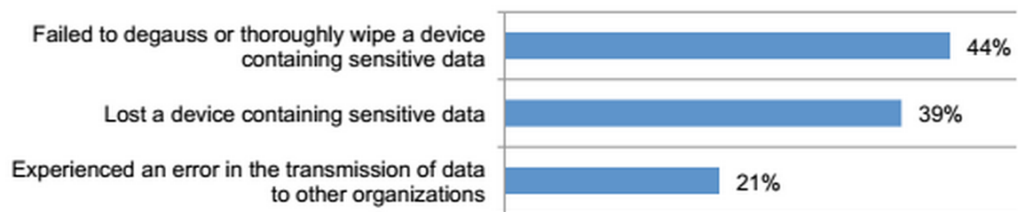


Malicious and Non-malicious

The two types of data breaches are non-malicious and malicious breaches. Non-malicious data breaches usually occur within the business unit or transit to a third party. Whereas malicious incidents most likely occur in an off-site or remote location where only 9% of the respondents said they are able to determine the location of non-malicious breaches (Ponemon Institute, 2013).

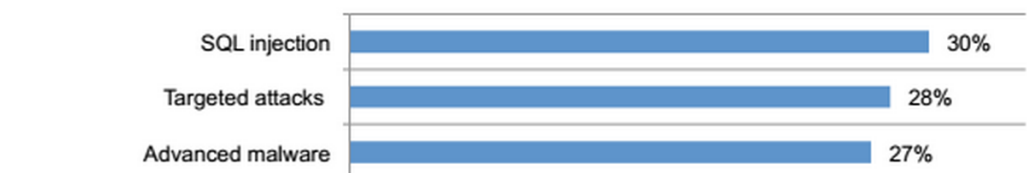
The figures below illustrate the top three non-malicious and malicious breaches.

More than one response permitted



Those breaches occur because of companies installing inferior data protection softwares. Data protection softwares are fundamental in grading companies.

More than one response permitted



Those breaches occur because of companies installing inferior data protection softwares. Data protection softwares are fundamental in grading companies.

1. SQL injection refers to injecting a code within websites or databases to retrieve information. Having loopholes in the operating systems could cause SQL injections.
2. Targeted attacks includes the the breach of sensitive information such as usernames, passwords, credit card details, etc. Companies that aggregate data in servers have a high risk of facing such malicious attacks

3. Advanced malware includes trojans, viruses, spyware, etc. Companies with inferior data protection softwares and poor encryption system face a high risk of such an attack.

APPENDIX 1.3

The Challenge of Anonymisation

Anonymisation has been criticised as being a weak instrument in safeguarding the identity of individual customers. Moreover, regulation regarding data minimisation also raises questions over effective privacy protection (Polonetsky & Tene, 2013), as the cost of data storage continues to decline creating a greater incentive for businesses to hold on to the data which should have otherwise been deleted (Holdren et. al, 2014). While regulation stipulates the anonymisation of data records, multiple applications capable of defeating this purpose currently exist and can be used legitimately, putting the identity of individual customers at stake. The process of anonymisation becomes inherently problematic when the quantity and range of data collected from the user reaches large proportions. Anonymisation has therefore been criticised as being a weak instrument in safeguarding the identity of individual customers.

Proposed Legislation and Data Minimisation

The debate around explicit consent and consumers ability to process legal documents before opting-in to services has given rise to proposals and implementation of systems which place greater power on the consumer's ability to control privacy preferences. PCAST, for example, proposes using a third party provider to set individual preferences which are then used for machine-reading of privacy policies. Thus, standards need to be implemented which enable an automated process for determining conformance to individual preferences. These systems termed "Trusted Data Format", are already beginning to be implemented in the information services sector (Holdren et. al, 2014).

Regulation regarding data minimisation also raises questions over effective privacy protection. The storage and collection of data will continue to grow since mining relies on gathering vast amounts of customer data for analysis (Polonetsky & Tene, 2013). As the cost of data storage continues to decline and businesses find efficient uses of historic data, there is great incentive to hold on to data which would otherwise be deemed necessary for deletion (Holdren et. al, 2014). This is especially the case as the benefits of data mining are predicted to experience significant growth (Polonetsky & Tene, 2013).

APPENDIX 1.4

Infinite Possibilities

With wearable devices, augmented value goes beyond superior customer service or flexible purchase terms. It is the companies ability to link information from several apps and create an ecosystem delivering highly relevant personalised messages (Kotler, 1960). By connecting to other platforms, technology companies can combine volunteered and observed data to develop inferred data enabling an omni-channel experience. Foursquare introduced “Swarm”, a location engine app that automatically registers the location of the user. The app also acts as a platform for linking other devices (Lapowsky, 2014). When connected to nutrition counselling, companies like Weight Watchers could develop personalised fitness plans for consumers based on their physical activity (Hajduk, 2013). Thus, as the number of platforms enabling syncing with wearable devices increase, opportunities become infinite.

APPENDIX 2.1

Primary Research Questionnaire and Validation

Wearable devices such as Nike Fuelband, Jawbone Up and Samsung smart watch are enhancing consumers lifestyle. These devices are gaining considerable adoption and this survey is about understanding the current and potential users attitude towards wearable devices. Please answer the questions as truthfully as possible. All responses will be anonymous and will only be used for academic purposes.

1. How familiar are you with the concept of wearable technology?
 - Very familiar
 - Somewhat familiar
 - Neither familiar nor unfamiliar
 - Somewhat unfamiliar
 - Very unfamiliar

Question Validation

Serves as a screening question. Respondents that do not know about wearable devices can not relate to the features and limitations and therefore are not fully capable of giving accurate answers. On the other hand, this analysis looks at those that are aware of wearables because the project scope includes existing consumers and potential consumers.

2. Did you know that personal information is collected from wearable devices?
 - Yes
 - No

Question Validation

To understand the percentage of users or potential users that are aware of data collection by companies.

3. Did you know that personal information collected from wearable devices can be shared between companies?

- Yes
- No

Question Validation

This question is different than the previous one because awareness of data collection by manufacturers' is different from awareness of the data being shared with 3rd parties.

4. How comfortable are you with sharing information with companies other than the maker of the wearable device:

- Very comfortable
- Comfortable
- Indifferent (Don't care)
- Uncomfortable
- Very uncomfortable

Question Validation

The critical insights is to find whether they are willing to share this information with 3rd party companies without feeling annoyed or distracted when unexpected messages are sent.

5. If you were to purchase a wearable device, which factors would you consider before making a purchase? Please tick up to 3.

- How much the device costs
- How it looks and feels
- The brand name
- The collection of private information
- The metrics it allows me to measure

Question Validation

This question will show whether privacy is key when purchasing wearable devices or it is not salient at the point of purchase.

6. Which of these aspects do you find compelling about using a wearable device?
Please rank each on a scale from 1 (very unattractive) to 5 (very attractive).

Benefit	1	2	3	4	5
Fitness and Health					
Stay Fit					
Live a healthier life					
Motivation to do more					
Reminder to be more active					
Social					
Be part of a community					
Trendy					
Challenge myself and friends					
Brand name					
Personalised Offers					
Very customized and relevant ads					

Question Validation

This question addresses the functional and emotional value of wearable devices.
This question will be used to create the intensity of value different consumers look for.

7. Please rate the following based on importance, 1 being the least important and 3 the most important.

- Fitness and Health
- Social
- Personalised offers

Question Validation

This question shows the importance of each utility aspect. This is helpful in creating the final grade of privacy for each respondent.

8. To receive fitness/health value, how comfortable are you with sharing the following information on a scale from 1 (not comfortable) to 5 (very comfortable). Fitness/health value (Includes: Stay fit, live a healthier life, motivation to do more, reminder to do more)

Types of Information	1	2	3	4	5
Personal Information (Name, Gender, Date of Birth and Email)					
Location					
Fitness Activity (Weight and Height, calories burned, Distance covered, type of sports)					
Food Consumption					
Health-related (Sleep cycle and heart rate)					
Mood					

9. To receive social value, how comfortable are you with sharing the following information on a scale from 1 (not comfortable) to 5 (very comfortable). Social value (Includes: Be part of a community, trendy, challenge myself and friends and brand name)

Types of Information	1	2	3	4	5
Personal Information (Name, Gender, Date of Birth and Email)					
Location					
Fitness Activity (Weight and Height, calories burned, Distance covered, type of sports)					
Food Consumption					
Health-related (Sleep cycle and heart rate)					
Mood					

10. To receive special offers, how comfortable are you with sharing the following information on a scale from 1 (not comfortable) to 5 (very comfortable). Special offers (Includes: Very customised and relevant ads)

Types of Information	1	2	3	4	5
Personal Information (Name, Gender, Date of Birth and Email)					
Location					
Fitness Activity (Weight and Height, calories burned, Distance covered, type of sports)					
Food Consumption					
Health-related (Sleep cycle and heart rate)					
Mood					

Question Validation

Questions 8, 9 and 10 deals with the degree of private information that consumers are willing to give up in return of a certain value. The question is set separate for each category of value because some consumers are willing to give up their information for functional value but not for social value. Results would provide insights on the privacy and utility trade-off that different consumers have.

11. Would you be willing to share more personal information collected from wearable devices with the manufacturing organisation in order to gain access to customised features, offers or discounts?

- Yes
- No

Question Validation

Now that respondents understand the case of privacy and utility. This question shows whether utility can be given in return of privacy being taken away.

12. The Google glass costs £1,200. Assuming you were to purchase this device, how much of your personal information are you willing to share? Please tick all that applies.

- Name, Gender, Dob, Email
- Location
- Fitness activity (weight and height, calories burnt, distance covered, type of sports)
- Food consumption
- Health-related (sleep cycle and heart rate)
- Mood

13. The Nike Fuelband costs £89. Assuming you were to purchase this device, how much of your personal information are you willing to share? Please tick all that applies.

- Name, Gender, Dob, Email
- Location
- Fitness activity (weight and height, calories burnt, distance covered, type of sports)
- Food consumption
- Health-related (sleep cycle and heart rate)
- Mood

Question Validation

Questions 12 and 13 will provide an insight on how price affects a users willingness to share their personal information.

14. What age group do you belong to?

- Below 18

- 18-25
- 26 - 35
- 36 - 45
- 46 - 55
- Above 55

15. What is your gender?

- Male
- Female

16. What is your current level of education?

- GCSE Diploma
- A-Level or equivalent
- Bachelor's degree
- Postgraduate degree
- Doctorate/professorial degree

17. What city do you currently live in? _____

Question Validation

Questions 14, 15, 16 and 17 are general demographic information that is crucial in understanding how privacy and utility tradeoff is different across different people. This could then help in recommending an additional layer when targeting consumers or creating loyalty programmes because we will be able to use the insights to provide specific attitudes based on which category a certain company's customers fall into.

APPENDIX 2.2

Cluster Analysis Findings (SPSS)

Dependent Variable: Q6 – Utility

Independent Variable: Q4 – Comfort with sharing information

Label	Cluster	Cluster	Cluster
Size	35% (43 respondents)	33.3% (41)	31.7%(39)
Inputs	Indifferent (72%)	Very Uncomfortable (63.4%)	Uncomfortable (100%)
	Reminder to be active (mean = 4.51)	Reminder to be active (mean = 3.10)	Reminder to be active (mean = 4.18)
	Motivation to do more (mean = 4.56)	Motivation to do more (mean = 3.24)	Motivation to do more (mean = 4.21)
	Stay Fit (mean = 4.37)	Stay Fit (mean = 3.41)	Stay Fit (mean = 4.23)
	Healthier life (mean = 4.35)	Healthier life (mean = 3.49)	Healthier life (mean = 4.10)
	Challenge myself and friends (mean = 3.65)	Challenge myself and friends (mean = 2.66)	Challenge myself and friends (mean = 3.26)
	Very Customised and relevant ads (mean = 2.91)	Very Customised and relevant ads (mean = 1.98)	Very Customised and relevant ads (mean = 2.31)
	Be part of a community (mean = 3.19)	Be part of a community (mean = 2.39)	Be part of a community (mean = 2.51)
	Brand name (mean = 3.30)	Brand name (mean = 2.66)	Brand name (mean = 2.67)
	Trendy (mean = 3.28)	Trendy (mean = 2.61)	Trendy (mean = 2.87)

Dependent Variable: Q14 – Age

Independent Variable: Q8 – Fitness/health value (stay fit, healthier life, motivation to do more, reminder to do more)

Label	Cluster	Cluster	Cluster
Size	55.1% (70)	28.3 (36)	16.5%(21)
Inputs	Age 18-25 (92.9%)	Age 18-25 (61.1%)	Below 18 57.1%
	Health Related (Sleep cycle, heart rate) (mean = 4.26)	Health Related (Sleep cycle, heart rate) (mean = 1.97)	Health Related (Sleep cycle, heart rate) (mean = 3.95)
	Food Consumption (mean = 4.07)	Food Consumption (mean = 2.22)	Food Consumption (mean = 4.05)
	Fitness Activity (Weight and Height, Calories Burnt, Distance covered, Types of sports) (mean = 4.37)	Fitness Activity (Weight and Height, Calories Burnt, Distance covered, Types of sports) (mean = 2.67)	Fitness Activity (Weight and Height, Calories Burnt, Distance covered, Types of sports) (mean = 4.00)
	Mood (mean = 3.69)	Mood (mean = 1.97)	Mood (mean = 3.76)
	Location (mean = 2.99)	Location (mean = 2.39)	Location (mean = 3.71)
	Name, Gender, DAB, E-Mail (mean = 2.91)	Name, Gender, DAB, E-Mail (mean = 2.91)	Name, Gender, DAB, E-Mail (mean = 2.91)

Dependent Variable: Q14 – Age

Independent Variable: Q9 – Social Value (community, trendy, challenge myself and friends and brand name)

Label	Cluster	Cluster
Size	63.2% (79)	36.8% (46)
Inputs	Age 18-25 (79.7%)	Age 18-25 (47.8%)
	Health Related (Sleep cycle, heart rate) (mean = 2.14)	Health Related (Sleep cycle, heart rate) (mean = 4.17)
	Food Consumption (mean = 2.28)	Food Consumption (mean = 4.11)
	Fitness Activity (Weight and Height, Calories Burnt, Distance covered, Types of sports) (mean = 2.30)	Fitness Activity (Weight and Height, Calories Burnt, Distance covered, Types of sports) (mean = 4.22)
	Mood (mean = 2.14)	Mood (mean = 4.02)
	Location (mean = 2.62)	Location (mean = 3.57)
	Name, Gender, DAB, E-Mail (mean = 2.85)	Name, Gender, DAB, E-Mail (mean = 3.33)

Dependent Variable: Q14 – Age

Independent Variable: Q9 – Special offers (very customised and relevant ads)

Label	Cluster	Cluster	Cluster
Size	50.0% (63)	31.0% (39)	19.0%(24)
Inputs	Age 18-25 (92.9%)	Age 18-25 (61.1%)	Below 18 57.1%
	Health Related (Sleep cycle, heart rate) (mean = 3.40)	Health Related (Sleep cycle, heart rate) (mean = 1.41)	Health Related (Sleep cycle, heart rate) (mean = 4.04)
	Food Consumption (mean = 3.68)	Food Consumption (mean = 1.49)	Food Consumption (mean = 4.00)
	Fitness Activity (Weight and Height, Calories Burnt, Distance covered, Types of sports) (mean = 3.67)	Fitness Activity (Weight and Height, Calories Burnt, Distance covered, Types of sports) (mean = 1.56)	Fitness Activity (Weight and Height, Calories Burnt, Distance covered, Types of sports) (mean = 3.96)
	Mood (mean = 3.27)	Mood (mean = 1.38)	Mood (mean = 4.00)
	Location (mean = 2.99)	Location (mean = 2.39)	Location (mean = 3.71)
	Name, Gender, DAB, E-Mail (mean = 3.30)	Name, Gender, DAB, E-Mail (mean = 1.82)	Name, Gender, DAB, E-Mail (mean = 1.79)

APPENDIX 2.3

Primary Research Interviews

1. Max Interview

About the participant

Company: Imperial College London

Sector: Wearable Technology

Name: Maximilian Doelle

Position: MSc Economics & Strategy for Business Student

Specialism: Wearable Technology Strategy

Tel: +447927184703

Email: maximilian.doelle13@imperial.ac.uk

Date and time of call: 7th of July 2014 at 1pm

Interview conducted by: Alanoud Alkaf and Dev Doowa

Interview duration: 90 minutes

Technique: Face-to-Face, Semi-structured interview

Introduction text for the research team

Consumers growing uncertainty over the safety of their personal data along with the continuous thirst of companies for information, creates a gap in the market. This gap opposes the customer-centric

approach objective and erodes customer-brand relationships.

The aim of the project is to provide Zeno Group (Marketing Agency) with a framework that addresses this gap and position it as a thought leader in this highly dynamic space from a communications

perspective. Considering the growth potential of wearables, a platform will be created through which privacy, security and value creation can be addressed.

The objective of the project is to understand the value that consumers put on privacy and the amount they are willing to waive for utility (value). A quantitative survey will be designed and analysed to develop a grading system of privacy and utility for different demographic-based segments. In addition, the objective is to understand how companies are upfront, honest and consumer-centric from the perspective of privacy of consumer information and utility that companies deliver.

In order to hone in on the customers perspective on wearables and privacy we have created the following survey:

https://qtrial2014.az1.qualtrics.com/SE/?SID=SV_6ujnyq9pdfvCfCB

However, we wish to gain insights into the companies perspective in order to develop the framework (i.e. match customer expectations with the companies)

The interview

Q1. What are the challenges that wearable manufacturers face regarding consumers privacy concerns?

“There are a few challenges that wearable manufacturers face, Misfit for example is a wearable device that allows you to take pictures of your food. And match this information with your level of activity. So thus, the app asks you if it can access your photo to enable this functionality. Therefore, although devices could access private information, companies tend to ask beforehand.

Also, Facebook now allows you to customise what you wish to share. And by this feature, Facebook could reduce consumers concerns.

However, Facebook bought Move in order to gain access to people’s activity levels who log into the app through FB log-in details. Consumers became very concerned. In this situations companies should educate users on the benefit of sharing information”

Q2. What type of unexpected information is collected by wearable devices?

“Solar panels around the city – as soon as you walk pass it sends a unique signal through wifi and can monitor congestion levels.

Flashlight GPS Scam – simple app, as soon as you turn on the flashlight it records your location data.

<http://www.techrepublic.com/blog/it-security/why-does-an-android-flashlight-app-need-gps-permission/>

Google Maps track consumers search, it then aggregates similar searches “e.g. people that want to go by car to a certain place”. This information is then used to understand and show traffic and congestion levels. There is an opt button for Google maps but consumers do not know about it”

Q3. What increases the risk of privacy breach?

“It depends on a number of factors. Of course, The more data uploaded on the internet, the higher potential for a breach. Therefore, for devices such as the misfit, the data is processed in the internet so consumers can access their activity trends from several devices. In this case, the challenge is to make it an end to end encryption.

Another factor is the operating system used. Operating systems are used to link wearables to other devices.

Tizen – used by Samsung

Android Wearable – WearOS

Pebble Operating System – new on by Google

Android operating system is an open source system. Google builds on Android. This is easily hackable. The danger however is that someone is able to breach it on a manufacturer level; they can see your GPS data and put things together. This is where it can get dangerous. A Major challenge would be to understand the encryption used by device manufacturer's.

It also depends on whether the data is stored and aggregated on servers. Misfit can give you information on your points and data. IT goes through their servers. The server keeps a local copy of the aggregated data. Also, SAP – right sharing scheme in Germany. Data stored in an “anonymised” form for statistical information to better understand consumers”

“If you’re a pig living in a barn and being fed everyday. Ask yourself if you’re a product” – Are we not secretly entering the deal and saying here use my data.

Q4. How can companies deal with privacy concerns?

“Most importantly, Companies need to tell consumers the benefits of the data collected.

Consumers should know what do companies do with their location and activity data collected and how does it add value to them. “Max likes this idea because he can receive customised services from third parties”.

Companies should outline is the terms and conditions What can they do with the data as a company. Being transparent is key to deal with the privacy challenge”

Q5. What are other uses of the sensory data collected?

“If you go to www.smartcitizen.me People voluntarily put up these sensors. The Purpose is to create a data platform where this data is openly shared and people can do their own research. For example, people are able to compare nitrogen levels in different cities or countries”

Q6. What are some examples of privacy breaches?

“Hackers hacked on e-commerce site, accessed usernames and password. They then used the same username and password to get into Tesco. It was not Tesco’s fault. Therefore there is Voluntary vs Involuntary (malicious, hacking) disclosure of data.

Snapchat had a data breach. If you put in the person's name, you could see their phone number. Someone wrote a program that allowed him to exploit the gap in the software. With those new technologies there is always a loophole and that is how hackers can win over the technology.”

Q7. What do you think is the future of privacy?

“In a study, people were offered a snickers bar for their password. 85% of them gave it because they assumed that the party would not know their username (which is in fact quite easy to obtain!). Therefore consumers do not highly value privacy when it was not salient.

2. Jawbone Interview

About the participant

Company: Jawbone

Sector: Consumer Electronics

Name: Bandar Antabi

Position: Vice President, Head of Special Projects

Tel:+4475217344

Email: bandar@jawbone.com

Date and time of call: Interviewed on the 10th of July 2014

Interview conducted by: Alanoud Alkaf, Devkaran Doowa, Magnus Eldevik

Interview duration: 65 minutes

Technique: semi-structured interview

Introduction text for the research team

The aim of the interview is to gain insight into Jawbone's market and customer strategy as well as the range of private information collected by the company to build customer profiles. Further interview questions in the interview also pertain to the data security which Jawbone has implemented to protect customer information. The insights gained from the semi structured interview will be applied to the Zeno Framework for assessing the tradeoff between utility and privacy in order determine Jawbone's performance. The interview was held with Bandar Antabi, Vice President and Head of Special Projects.

The interview

1. How does Jawbone brand position itself relative to competition?

"We are in the business of improving people's lives. We want to build the first 24 hour contextualised service which makes life easier by providing solutions for self-improvement. Unlike Smart watches and glasses; UP is worn 24/7. Thus, the data

gathered is significantly more than other wearable devices which allows the company to better”

2. Who is Jawbone’s target market?

“We are targeting people who take an interest in their health and want to live a more active lifestyle. It does not just have to be the professional athlete, it can be someone who wants to start being more active and is looking to get solutions on what the best approach is to improving their life. So far we have over a trillion steps in the system. A hundred million hours of sleep in the system. From this we have gained a lot of insight into different markets. For example, in the UK, people move more than in the US. Users in Japan an hour and twenty minutes less. Men tend to sleep 20 mins less than women around the world.”

3. How does it affect consumers health and fitness?

“We basically get customers to opt-in to our services and begin by monitoring their normal behaviour. The loop of data is then analysed and areas are detected where customers can improve or root causes can be detected. The customer then has a baseline from which they can begin to understand more about their own behaviour and compare their own progress. We then also tailor programmes for improving their performance or health. This process of self-improvement creates a high level of engagement with the Jawbone and has netted us a remarkably high retention rate of 80% with 20 opens per day. Stanford published a wearable technology article in the journal of medical sciences using Jawbone to monitor biometric data from different patients.”

4. Where do you see wearables made by Jawbone in the future?

“Hardware is not the sole focus, it is rather the medium to deliver the value which we wish to create for the customer and the outlet through which data is fed into the ecosystem of software. The focus is on data and software as well. Through creating an open ecosystem which runs parallel to Jawbone’s own servers we analyse data

from millions of customers to detect trends, design programmes and create feedback. Jawbone has built a culture around data where granular aspects of life can be quantified, analysed and improved. We are effectively building the first contextualised 24 hour data set around you through monitoring: Activity, Biometrics and Identity data.”

5. How will wearable technology change in the future?

“The revolution coined “Internet of you” creates an interconnected environment where it will be challenging to internalise the design of all different forms of software. For this reason we opened up their API for other apps to feed into their UP platform. Jawbone will therefore function as an interface between the connected home and the user to make technology adapt to you instead of having to navigate devices yourself.”

6. What is the range of information that Jawbone collects from the device?

“We collect a range of information such as biometric, activity and health related data, motion, heart rate, calories consumed.”

7. There are a range of operating systems such as Tizen and WearOS. What operating system does Jawbone use to link the device to the app?

“We have the Up system which is an ecosystem of apps developed specifically for the Jawbone. These are available for android and iOS phones where consumers can interact with services and monitor their own progress.”

8. Where does the data processing take place, is it on the iPhone, device, computer or over the Internet?

“Processing occurs in the band itself, the user’s smartphone, in the cloud and on individual servers from companies which link into Jawbone’s systemsup.”

9. How do you protect your software?

“We have our own operating system which uses end-to-end encryption to ensure that data is not vulnerable to outside parties. We have opened our API’s but have a strict protocol and quality control mechanism for ensuring these parties comply with our policy.”

10. How do you protect consumers private information?

“Jawbone offers an opt-in directly to our system to collect richer data and return greater detail to customers (as opposed to an opt-out model which the majority of companies are doing). We also offer customers the option to have their data deleted at any time. The value proposition is built on transparency with users.”

11. To what extent do Jawbone’s consumers know about the type of information collected?

“Jawbone gives the user all the tools to manage their own data. They do not own any of the data.”

12. If the information collected is saved on certain servers, what kind of data protection software is used?

“Data is constantly fed through the device and aggregated in the cloud in order to create smart data with contextualised messages (creates value through recommendation and tailored programmes which are designed specifically to the individual in order to push them towards a healthier life and fulfilling day).”

13. What functional value do you provide to the users of Jawbone?

“We collect data on the user’s activity and allow them to measure, monitor and compare this information for self-improvement. We also give recommendations for how they can better reach their goal. The messages are meaningful and intimate with each individual which creates stickiness.”

14. What emotional value do you provide to the users of Jawbone?

“The software experience creates a unique emotional bond between the customer and the device. The user experience is unique to the individual and can be completely different on a per person basis. We have received testimonials with customers claiming to have seen their lives greatly improved.”

15. Do you provide unexpected/augmented value (contextualised messages) to consumers?

“Guarantees were offered where customers were given a refund if they didn’t like the product (this was done following a faulty start where they had quality issues). This established trust with new customers and also goodwill where Jawbone strengthen their image of being all about improving the lives of the customer (this guarantee is still part of the value proposition). We also have a range of standalone software such as CoffeeUp which plots your caffeine intake across a timescale to monitor consumption levels and improve wellbeing. It is not just limited to coffee but all sources of caffeine such as headache medication. This creates contextualised messages for improving well being from the data analysed.”

16. What kind of data does Jawbone share with third parties (volunteered, observed, inferred)?

“We use a team of data scientists (background in computer science, statistical mathematics, algorithm scientists) who analyse the aggregated data and produce unique reports with trends from which new insight is born such as, new software development, extensions, programme recommendations, national statistics based on a range of different factors with demographic data as a basis. They basically combine micro data from individuals and pair it through for example cross tabulation with macro data to gain an overview of different user groups.”

“Up has become an ecosystem for data exchange pushed through the cloud and updated in our main system. The individual app developers need to abide by Jawbone’s data deletion clause in order to ensure consistency. This is vital because we want to create trust not a commerce platform for third party providers.”

3. CitiZen Science Interview

About the participant

Company: Cityzen Sciences

Sector: Wearable Technology

Name: Gilbert REVEILLON

Position: Vice President, Head of Special Projects

Specialism: Marketing Strategy

Tel: +33685086013

Email: greveillon@cityzensciences.fr

Date and time of call: 12 July 2014, 14 July 2014

Interview conducted by: Alanoud Alkaf

Technique: Telephone and Email

Introduction text for the research team

We are a group of 6 members studying Masters in Strategic Marketing at Imperial College London. We are currently working on a consulting project that analyses consumers attitude towards privacy and how much they are willing to give up for a certain utility in the context of wearable technology.

The purpose of the meeting is to understand the steps that Cityzen Sciences takes to be more upfront and transparent about the information collected and the amount of utility it provides to current and potential consumers in order to build sustainable behavioural loyalty.

The interview

Q1: What is the range of information is collected by the shirt?

“The D-Shirt integrate following sensors

2+1 leads ECG

Center of mass activity through Inertial Measurement System

Geolocation

Altimetry”

Q2: There are a range of operating systems such as Tizen and WearOS. What operating system do you use to connect the shirt to other devices?

2 versions of embedded SW in the Gateway(connect the shirt to external world).

Free RTOS only

Free RTOS + embedded JVM

Q3: Where does the data processing take place, is it on the iPhone, computer or over the Internet?

“Data processing takes place in the Gateway in real time and over the internet for Analytics.”

Q4: How do you protect your software?

Encryption

Q5: How do you protect your consumer information and if the information collected is saved on certain servers, what kind of data protection software is used?

“Encryption in the Gateway”

Data transmission to the CityZen Data platform is encrypted using SSL (using Perfect Forward Secrecy).

At the storage layer, all metadata about Geo Time Series are encrypted using AES with 256bits keys. Data on our hard drives is not sufficient to identify Geo Time Series without the decryption key. All keys used on the Cityzen Data Platform are

kept in a security module and can only be released by authorised personnel at application launch time.

Data access on the Cityzen Data Platform is controlled by the use of cryptographically secure OAuth tokens. Tokens can be revoked at any time. Data access is tracked in an audit log”

Q6: Do you provide unexpected/augmented value (contextualised messages) to consumers?

“In real time through Smartphone application we provide a lot of indicators (see before) and geolocation coming from the Gateway (embedded), most of them are coming from data fusion (several sensors are used).

All the indicators are calculated according to user parameters and sport activity so there are fully contextualised (who, where, when). We also provide a channel for brands to consumer communication through this app”

4. David Keene (Google) Interview

About the participant

Company: Google

Sector: Internet/Computer Software/Telecom

Name: David Keene

Position: Head of Marketing Northern Europe

Date and time of call: 17 July 2014

Interview conducted by: Margherita Capitanio, Alanoud Alkaf, Devkaran Doowa, Magnus Eldevik

Interview duration: 1 hour 15 minutes

Technique: Semi-structured Interview

Introduction text for the research team

The aim of the interview was to gain insight into the current marketing strategy of Google Glass and the infrastructure used to protect data transmitted from the device. The insights gained from the interview were applied to the framework developed by the research team to grade Google Glass performance in providing privacy and utility. The interview was arranged at the Google office in London, where a semi-structured interview was conducted with David Keene. As the Head of Marketing in Northern Europe, Mr. Keene's responsibilities ranged between overseeing product development to formulating the go-to-market strategy for Glass.

The interview

1. How does Google Glass brand position itself relative to competition?

"Google Glass has a functional positioning which is focused on making technology frictionless, whereby everything is hands free, mobile and connected to the user's mobile, cloud and individual network. It is positioned as a device where technology goes out of the way and becomes more efficient."

2. What is Google Glass' marketing strategy?

"Glass is currently focused on building an appropriate user case through demonstration, the use of the device itself is unfamiliar to the majority of the public who have yet to see a use case for it. The strategy is to educate consumers to the range of applications for which glass can be used to illustrate how useful the technology can be and to get people to change their behaviour. The product itself is still in a very early stage and is constantly being refined and designed to look more subtle. We want to build network effects which is hugely important for getting app developers to commit towards building the Glass ecosystem."

4. How does Google intend to change consumer lifestyle with Google Glass?

"Glass intends to make the whole concept of technology more assistive in our daily lives rather than something we manage and have to navigate through to get to a certain end point. By interacting with the device through voice command and

eventually further down the line eye control - we want to make technology more seamless in behaviour. Rather than interrupting your behaviour by glancing down at a screen we want to allow people to interact with surroundings and the machine itself. We have made great advancements to machine learning in the past and are continuing to push towards it in the future". -

David Keene proceeded to demonstrate machine learning by talking to his mobile phone.

David Keene - "Google Now - who is the current president of the United States?"

Google Now - "Barack Obama is the 44th President of the United States of America and was inaugurated on June 20th 2009."

David Keene - "who is his wife?"

Google Now - "Michelle Obama is the first lady and wife of President Barack Obama"

5. How does it affect consumers health and fitness?

"Glass has a lot of potential to make an impact in the sports sector where they can assist athletes in reading different metrics for of their performance in real time. Glass can also be used as a navigational tool for pedestrians and cyclists alike. There are also use cases for different industries such as factory work where employees scan barcodes and monitor stock levels"

6. Where do you see wearables made by Google in the future?

"I see the technology becoming a lot smaller, smarter and sleek in design. We would like to reduce the design to contact lenses which we are also currently developing."

7. How will wearable technology change in the future?

"Wearable technology will become more contextually driven to the individual where they deliver relevant information in real time and function alongside daily routines of the individual".

8. What is the range of information that Google collects from Google Glass?

"It's not collecting information at that point it's more using information which is already in the cloud. Glass is configured over your your google account so it is basically just like logging into gmail."

9. There are a range of operating systems such as Tizen and WearOS. What operating system does Google use to link the device to the app?

"Glass uses Android to connect to the Google system, we realised that if we want to be on the forefront of ubiquitous computing we have to open our system to app developers who will help us in shaping the user experience. Only through following this strategy can we provide robust use cases for vastly fragmented user profiles".

10. Where does the data processing take place, is it on the iPhone, Android, computer or over the Internet?

"Processing is happening in the cloud, connected via Bluetooth, wifi or 3G, allows you to engage with services in the cloud".

11. How do you protect your software?

"Glass follows our strict data encryption practices. Data encryption happens at the device in transit, in passing different points, at end points, we use chrome browser's safety features. All the encryption practices which apply to gmail are also used for Google Glass. We also have large teams monitoring bad websites to detect malicious websites and warn users of any danger or to be proactive. Third parties have to become certified Tested and checked which means we are actively engaging with organisations on the web".

12. To what extent do Google consumers know about the type of information collected?

“When you define identity you want to compile the tracking of tasks for context to be maintained, your history is maintained according to your search history. Glass does not do anything which consumers are not already familiar with from using Google search. They have the option to control the collection of information and their history”.

13. What functional value do you provide to the users of Google Glass?

“Glass offers a range of functions which users can engage with. Taking photos, playing games, handling text messages, reading emails, surfing the web, navigation etc. Glass is basically developed as an open ecosystem which thrives as android developers develop the market”.

14. What emotional value do you provide to the users of Google Glass?

“Our focus is on getting consumers familiar with the technology first and foremost. We also engage in some fashion marketing to make it more fashionable and aspirational.”

15. Do you provide unexpected/augmented value (contextualised messages) to consumers?

“Currently the idea of receiving a coupon based on augmented reality is still a far reach. you could opt in to a third party app to receive special offers but the main focus is on getting the technology running the way we intend it to primarily function. The business model of google is to monetizing late, basically building solutions around the platform which we are doing with Glass. Pay per glance is not something we are actively considering for monetising glass. We have a range of options which we are examining right now”.

16. Where do you see customer privacy in the future? Will people eventually become more or less concerned overtime?

“There needs to be a clear governance model around data ownership for consumers, we expect a trifecta of high standards, free and tailored services free of privacy concerns. That is difficult to pull off without a range of data available to you. So the question is who really owns this data and in what ways can this information be used to the benefit of the consumer. Its not an issue of legislation it's more governance which is fragmented and local. This makes it difficult to assign responsibility over what happens to data which is transferred across borders. The question is how do we deal with the flow of information in terms of an applicable framework for cross border protection?”

17. What kind of data does Google share with third parties (volunteered, observed, inferred)?

“Glass follows the same policy that all other Google services is subject to where no data is shared with third party companies unless the consumer has given explicit consent for us to do so.”

APPENDIX 2.4

Primary Research Analysis Methodology

SPSS and Qualtrics filter features were used to cluster and analyse homogenous segments. For each segment a persona was described using the perceived benefit attractiveness, comfortability in sharing information, the importance of the three different utility types, the features that are most important at the point of purchase and the demographics they belong to.

For each segment, the utility score was calculated by taking the average of the mean for each feature listed in question 6 of the survey. To minimise bias, consumers were indirectly asked about the value they put on their privacy. Instead of asking “How much do you value your privacy”, we asked “How comfortable are you sharing different types of information”. The privacy score was calculated by subtracting the average of the mean values for all the types of information collected in question 8, 9 and 10 from 5. Therefore, a respondent that is very comfortable in sharing information will receive a low score because they do not highly value their privacy. Through this subtraction step, the utility and privacy score represent the consumers’ value attributed to privacy or utility. The purpose of splitting the question to three was to understand how consumers willingness to share information differ across different benefits.

APPENDIX 3.2

Persona Identification Questionnaire

Wearable devices such as Nike Fuelband, Jawbone Up and Samsung Smartwatch are enhancing consumers' lifestyle. These devices are gaining considerable adoption and this survey is about understanding the current and potential users attitude towards personal information collected from wearable devices. Personal information includes name, email, location, weight, height and heart rate. Please answer the questions as truthfully as possible. All responses will be anonymous and will only be used for academic purposes.

1. How familiar are you with the concept of wearable technology?

- Very familiar
- Somewhat familiar
- Neither familiar nor unfamiliar
- Somewhat unfamiliar
- Very unfamiliar

2. Which of these aspects do you find compelling about using a wearable device? Please rank each on a scale from 1 (very unattractive) to 5 (very attractive):

	1	2	3	4	5
Stay fit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Live a healthier life	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Motivation to do more	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Reminder to be more active	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Be part of a community	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Trendy	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Challenge myself and friends	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Brand name	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Very customised and relevant ads	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

3. Please rate the following based on importance, 1 being the most important and 3 the least important. Please click and drag to order the options.

Fitness and Health

Social

Personalised offers

4. To receive **fitness/health value**, how comfortable are you with sharing the following information on a scale from 1 (not comfortable) to 5 (very comfortable). Fitness/health value (Includes: Stay fit, live a healthier life, motivation to do more, reminder to do more).

	1	2	3	4	5
Name, Gender, Date of birth, Email	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fitness Activity (Weight and Height, Calories burnt, Distance covered, Type of sports)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Food Consumption	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Health-related (Sleep cycle and heart rate)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mood	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

5. To receive **social value**, how comfortable are you with sharing the following information on a scale from 1 (not comfortable) to 5 (very comfortable). Social value (Includes: Be part of a community, trendy, challenge myself and friends and brand name)

	1	2	3	4	5
Name, Gender, Date of birth, Email	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fitness Activity (Weight and Height, Calories burnt, Distance covered, Type of sports)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Food consumption	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Health-related (Sleep cycle and heart rate)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mood	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

6. To receive **special offers**, how comfortable are you with sharing the following information on a scale from 1 (not comfortable) to 5 (very comfortable). Special offers (Includes: Very customised and relevant ads)

	1	2	3	4	5
Name, Gender, Date of birth, Email	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Location	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fitness Activity (Weight and Height, Calories burnt, Distance covered, Type of sports)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Food consumption	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Health-related (Sleep cycle and heart rate)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mood	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

7. What age group do you belong to?

- Bellow 18
- 18 - 25
- 26 - 35
- 35 - 45
- 46 - 55
- Above 55

8. What is your gender?

- Male
- Female

9. What is your current level of education?

- GCSE Diploma
- A-Level pr equivalent
- Bachelor's degree
- Postgraduate degree
- Doctorate/professional degree

10. What city in England do you currently live in?

Persona Identification Methodology

To identify which persona the client's customer fall into, Zeno Group could send this questionnaire to the customers. Question 2 is related to the consumer perception on the device benefit. Questions 4, 5 and 6 study consumer perception towards sharing personal information. The same calculation explained in Appendix 2.4 must be followed to derive the privacy and utility scores. Demographics are essential in personalised the customer acquisition strategy.

APPENDIX 3.1

Privacy-Utility Scorecard

Company Privacy vs. Utility Scorecard

Factor	Component	Defintion	Score	Explanation
Privacy	Quantity	The amount of data collected and saved from wearable devices. This includes: contact details, fitness and health information, in-app behaviour and location. Companies should not collect information that they do not need to deliver valuable communications.	/5	
	Transparency	The degree to which a company informs consumers about the information collected and explain the value added to consumers. Privacy policy should be clear and concise to ensure easy consumer reach and education.	/5	
	Confidentiality	The amount of data that can disclosed without consent of consumer. Information should be used for limited, specifically stated purposes. Privacy policy should include the type of information collected, third parties shared with, reason for sharing and benefits of sharing.	/5	
	Data Protection	The degree to which information collected is kept safe and secure (Data Protection Act, 1998). There are three components to data protection for wearable devices: Security of operating system, location of data processing and storage and aggregation of data.	/5	
	Salability	The act of selling the information collected to 3rd parties. Grading will not only take into considering if consent was taken but also the amount of information sold and the types of companies it was sold to.	/5	
Utility	Functional value	The second layer of the brand dimensions of differentiation. In includes: fitness tracking, sleep cycle, alarms, durability and design of the wearable device relative to competition.	/5	
	Emotional value	Emotional value is derived from the brand image and communication messages. It includes: Feeling trendy, active or health-conscious person.	/5	
	Augmented value	The third layer of the brand dimensions of differentiation. It includes delivering unexpected value that differentiates a company in the market. It could includes using perceptive design to deliver targeted and real-time communications.	/5	

APPENDIX 3.2

Grading System

Grading System

Component	1	2	3	4	5
Quantity	Company collects and aggregates volunteered data. It also collects information required to send realtime offers and discounts (Observed data). Additional information includes: Date of birth, location, in-app behaviour and mood of the day.	Company collects and aggregates information that is necessary for the functionality of the device (Volunteered data). It includes: name, gender, email, height, weight, calories burned, distance covered, types of activities, sleep cycle and food consumption.		Company collects information that is necessary for the functionality of the device (Volunteered data) but does not aggregate it. It includes: name, gender, email, height, weight, calories burned, distance covered, types of activities, sleep cycle, food consumption and social media platforms.	
Confidentiality	Considerable disclosure of personal information or data to third party without consent (illegal under the Data Protection Act 1998).	Some disclosure of personal information or data to third party without consent. It includes: name, gender, email, height, weight, calories burned, distance covered, types of activities, sleep cycle and food consumption.		None/Limited disclosure of personal information or data to third party without consent	
Transparency	Complex and overwhelming terms and conditions through relevant communication channel.	Clearly stated terms and conditions through relevant communication channel.		Clearly stated terms and conditions with an explanation of the benefits provided through collection of personal information.	
Data Protection	Company does not use operating system with end-to-encryption of data feature. It processes data in the internet, aggregate data in servers and installs inferior data protection software.	There are four aspects of data protection. Company has 2 out of 4.		Company does use operating system with end-to-encryption of data feature. It processes data in the computer, does not aggregate data in servers and installs superior data protection software.	
Salability	Company sell inferred (processed) data which combines both volunteered and observation data to prove contextually relevant information.	The sale of raw volunteered and observation data.		No sale of data.	
Functional Value**	There are 10 features that deliver distinct functional value. Company deliver 2 out of 10.	There are 10 features that deliver distinct functional value. Company deliver 5 out of 10.		There are 10 features that deliver distinct functional value. Company delivers 10 out of 10.	
Emotional Value	There are 5 emotional benefits delivered by wearable devices. Company provides none.	There are 5 emotional benefits delivered by wearable devices. Company provides 3 out of 5.		There are 5 emotional benefits delivered by wearable devices. Company provides 5 out of 5.	
Augmented Value	There are 4 augmented benefits delivered by wearable devices. Company provides none.	There are 4 augmented benefits delivered by wearable devices. Company provides 2 out of 4.		There are 4 augmented benefits delivered by wearable devices. Company provides provide 4 out of 4.	

**Assume all benefits are equally weighted

APPENDIX 4.1

CityZen Science – Case Application

CityZen Sciences is a French company that took fitness tracking from wrists to textiles. Through the use of micro-sensors that are embedded in shirts, CityZen Sciences was able to create the Digital Shirt (D-Shirt). It tracks activity data, user running or biking speed and acceleration, altimeter, heart rate, cardiovascular stress, temperature and geolocation. Just like other wearable devices, the D-Shirt could be connected to smartphones to enable real-time tracking of activity and fitness progress. On top of that, CityZen Sciences extends the devices to a platform where third party companies could link to and provide customers an augmented value.

Cityzen Sciences taps into a white space in the fitness market by targeting professional and amateur athletes. This positioning creates a unique value proposition for fitness savvy customers and football clubs. In fact, the D-Shirt could revolutionise the football market, as coaches could track players and determine when they are tired or stressed. Thus, the combination of smart textiles and unique a target market puts Cityzen Sciences at a breakthrough positioning in the wearables market.




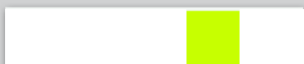




Cityzen Sciences Privacy vs. Utility Scorecard

Factor	Component	Defintion	Score	Explanation
Privacy (2.6)	Quantity	The amount of data collected and saved from wearable devices. This includes: contact details, fitness and health information, in-app behaviour and location. Companies should not collect information that they do not need to deliver valuable communications.	1	Cityzen Sciences collects volunteered data required for activity and fitness tracking. It also collects observed data such as geolocation information through the embedded GPS tracker. All information is also aggregated in the cloud.
	Transparency	The degree to which a company informs consumers about the information collected and explain the value added to consumers. Privacy policy should be clear and concise to ensure easy consumer reach and education.	2	All information collected is clearly outlined in the home page of the website. However, the value delivered is not clearly outlined in the website.
	Confidentiality	The amount of data that can disclosed without consent of consumer. Information should be used for limited, specifically stated purposes. Privacy policy should include the type of information collected, third parties shared with, reason for sharing and benefits of sharing.	4	Cityzen Sciences does not disclose speed, physio and race course information without consent. However, information is shared by 3rd party after implied consent.
	Data Protection	The degree to which information collected is kept safe and secure (Data Protection Act, 1998). There are three components to data protection for wearable devices: Security of operating system, location of data processing and storage and aggregation of data.	4	Cityzen Sciences Data want to create the best data management platform. Information is collected and processed in the Gateway and analysis are performed in the cloud. Cityzen Sciences uses Free RTOS + embedded JVM to connect the gateway to other devices. Although processing in the cloud and aggregates and fusses data in the cloud, data transmission to the Cityzen data platform is encrypted using SSL. At the storage layer, all metadata are encrypted using AES with 256bits keys. Data on hard drives is not sufficient to to be analysed without the decryption key. All keys used on the Cityzen Data Platform are kept in a security module and can only be released by authorised personnel at application launch time. Data access on the Cityzen Data Platform is controlled by the use of cryptographically secure OAuth tokens. Tokens can be revoked at any time. Data access is tracked in an audit log.
	Salability	The act of selling the information collected to 3rd parties. Grading will not only take into considering if consent was taken but also the amount of information sold and the types of companies it was sold to.	2	Cityzen Sciences strives to create an ecosystem where other companies could connect to and reach consumers effectively. An app download implies that consumers are willing to share information with 3rd parties.
Utility (3.0)	Functional value	The second layer of the brand dimensions of differentiation. In includes: fitness tracking, sleep cycle, alarms, durability and design of the wearable device relative to competition.	5	To best reach athletes, Cityzen Sciences provides the ultimate functional features and benefits. The cardiovascular and acceleration tracking is very customised to athletes.
	Emotional value	Emotional value is derived from the brand image and communication messages. It includes: Feeling trendy, active or health-conscious person.	1	Given that the D-Shirt is still a very new product, the focus is on the functional benefit. Advertisements does not show any social benefits and the shirt design is not meant to be a fashion statement.
	Augmented Value	The third layer of the brand dimensions of differentiation. It includes delivering unexpected value that differentiates a company in the market. It could includes using perceptive design to deliver targeted and real-time communications.	3	By infusing all the types of data collected and information collected from 3rd party apps, Cityzen Sciences will enable partnered companies to deliver contextualised messages. Given that the product is still very new, purchasing terms are not outlined yet.

(Reveillon,2014)

Cityzen Sciences | Part Gap Analysis and Recommendations

Privacy = 2.6 Utility = 3.0

Target Market	GAP (LITMUS)	Communication Strategy
The Skeptic Privacy = 4.0 Utility = 2.8	Privacy = -1.4  Utility = -0.2 	The company communications strategy should focus on educating consumers about the safety and security of their personal information. Although Cityzen are strong in data protection; they currently lack customer transparency on how this data can help deliver value. Cityzen should use content marketing to promote the functional benefits of their products and use their star performers to advocate their brand through word-of-mouth (Rowles, 2014). At the same time, offline marketing activities such as print, magazines and newspaper may be an appropriate channel of communication given the demographic makeup of the customer segment.
The Rational Privacy = 2.54 Utility = 3.1	Privacy = 0.06  Utility = -0.1 	The company communications strategy should focus on increasing customer awareness about the functional benefits of their products. Given Cityzen's strength in customisation of cardiovascular and acceleration tracking technology, marketing efforts (i.e. website, social media, PPC, email) should highlight these functional attributes that athletes sought after. Content marketing should focus on case studies and interactive demos that demonstrate how the product can improve athletic performance. It is recommended that CityZen Sciences targets this consumer segment.
The Curious Privacy = 1.47 Utility = 3.95	Privacy = 1.13  Utility = -0.95 	Cityzen should focus their communication strategy on how to build an emotional bond with the customer. Since, 'the curious' are intrigued by new experiences, Cityzen have to constantly update its sources of delight by providing unexpected benefits to customers (Merlo, 2014). For example, new software features will keep them hooked and may lead to positive word-of-mouth.
The Star Performer Privacy = 0.78 Utility = 4.17	Privacy = 1.82  Utility = -1.17 	Cityzen should constantly engage with star performers by offering vouchers or discounts for sporting events or concerts. By providing valuable and relevant content (i.e. sports news, new technology) through email and social media this may enhance the level of brand advocacy. Moreover, crowd-sourcing and online competitions this may lead to higher levels of customer participation and loyalty (Merlo, 2014).

Google Glass: Case Application

Google Glass was released in February 2013 and has been available in retail stores since April 2014 at a price of \$1500. Using an optical head-mounted display users give commands through a microphone mounted on the side of the frame, which also contains a navigational pad. The software was built using the Android operating system with the intention of creating an ecosystem for independent developers to contribute towards shaping the user experience. Data is processed in the cloud using wifi and bluetooth to allow users to interact with their surroundings via augmented reality.

Google Glass is currently in the process of shaping the market, by targeting innovators with a purely functional positioning focused on enabling consumers to navigate their use of technology in a hands-free manner. Google's main priority is to prove a robust use case for the technology to propel widespread adoption. The integration of augmented value is still outstanding as Android developers have yet to contribute towards building the glass ecosystem. Contrary to portrayal in the media, Glass is subject to a strict privacy policy which does not disclose information without the users consent.









Google Glass Privacy vs. Utility Scorecard

Factor	Component	Defintion	Score	Explanation
Privacy (2.8/5)	Quantity	The amount of data collected and saved from wearable devices. This includes: contact details, fitness and health information, in-app behaviour and location. Companies should not collect information that they do not need to deliver valuable communications.	1	Information collected is all about creating an identity. It collects basic gmail account details and all actions done by users; including search, navigation, location and 3rd party app data (e.g. Facebook or Fitness apps).
	Transparency	The degree to which a company informs consumers about the information collected and explain the value added to consumers. Privacy policy should be clear and concise to ensure easy consumer reach and education.	4	Google has a very clearly outlined privacy policy. They indicate all information collected and the benefits of collection. However, the value is very general which makes it harder for consumers to relate to.
	Confidentiality	The amount of data that can disclosed without consent of consumer. Information should be used for limited, specifically stated purposes. Privacy policy should include the type of information collected, third parties shared with, reason for sharing and benefits of sharing.	4	It is clearly outlined in the privacy policy that Google does not disclose information without consumers consent. However, downloading a 3rd party app implies consent for the follow of information from google to 3rd party companies.
	Data Protection	The degree to which information collected is kept safe and secure (Data Protection Act, 1998). There are three components to data protection for wearable devices: Security of operating system, location of data processing and storage and aggregation of data.	3	All data is processed and aggregated in the cloud, instead of the Glass itself in order to take context from one step to another. Google uses an Android OS, which is an open platform. The OS used and the processing location, makes data more vulnerable to attacks. Yet, Google uses a double encryption system, at-rest and in-transit to ensure data protection. Google also has a team for data protection and security to ensure that privacy is not breach.
	Salability	The act of selling the information collected to 3rd parties. Grading will not only take into considering if consent was taken but also the amount of information sold and the types of companies it was sold to.	2	Google does not sell information to 3rd parties. However, information is indirectly shared with other companies that are part of the Google Glass platform.
Utility (2.6/5)	Functional value	The second layer of the brand dimensions of differentiation. In includes: fitness tracking, sleep cycle, alarms, durability and design of the wearable device relative to competition.	5	Google Glass is purely a functional product. It provides benefits ranging from navigation and engine search to fitness and gaming.
	Emotional value	Emotional value is derived from the brand image and communication messages. It includes: Feeling trendy, active or health-conscious person.	2	Google is not meant to be a fashion statement or aspirational. However, the device is taking one step into the social value through partnership with Luxottica.
	Augmented Value	The third layer of the brand dimensions of differentiation. It includes delivering unexpected value that differentiates a company in the market. It could includes using perceptive design to deliver targeted and real-time communications.	1	Google Glass follows the Youtube business model, it is about monetising late. Google Glass by itself does not deliver any augmented value. Yet, in the future, it depends on 3rd party companies to create an augmented experience through contextualised advertising using the Google Glass platform. Google Glass also does not have any guarantees or flexible purchasing terms.

(Keene,2014)

Google Glass Analysis and Recommendations

Privacy = 2.8 Utility = 2.6

Target Market	GAP (LITMUS)	Communication Strategy
The Skeptic Privacy = 4.0 Utility = 2.8	Privacy = -1.2  Utility = 1.2 	The company communications strategy should focus on educating consumers about how Google Glass protects the confidentiality of their personal information. By being transparent about their customer 'opt-in' approach, this will increase customer trust and improve their willingness to adopt. Marketing efforts should highlight the functional attributes of the device which provides users with seamless and relevant information. Content marketing efforts should focus on educating and convincing users through a mix of infographics, interactive demos, and case studies relating to product usage (Bosomworth, 2012). In addition, offline marketing activities such as print, magazines and newspaper may be an appropriate channel of communication given the demographic makeup of the customer segment.
The Rational Privacy = 2.54 Utility = 3.1	Privacy = 0.26  Utility = -0.5 	The company communications strategy should focus on increasing customer awareness about the functional value of Google Glass. They should highlight how the product provides users with 'hands-free' access to information when and where they need it. Content marketing should focus on providing technical product features, interactive demos and case studies in order to convince users on a rational level (Bosomworth, 2012). It is recommended that Google targets this consumer segment.
The Curious Privacy = 1.47 Utility = 3.95	Privacy = 1.33  Utility = -1.35 	Google should focus their communication strategy on how to build an emotional bond with the customer through aspirational messages. Through their association with Luxottica, they can improve their lifestyle positioning. Since, 'the curious' are intrigued by new experiences, the company have to constantly update its sources of delight by providing unexpected benefits (Merlo, 2014). This may be achieved through updated software features or aesthetic enhancements. Email and social media marketing may be used to provide inspirational content such as viral videos, games and competitions. By updating sources of delight, the customer will continue to feel engaged.
The Star Performer Privacy = 0.78 Utility = 4.17	Privacy = 2.02  Utility = -1.57 	Google should provide valuable, relevant and exclusive content to star-performers in order to build brand advocacy. Through crowd-sourcing and online competitions this may lead to higher levels of customer participation and loyalty (Merlo, 2014). Jawbone should provide a platform for users to share their stories with others.

Jawbone Up: Case Application

Jawbone develops and markets wearable technologies and audio devices that are of high technical innovation with a trendy design. However, in the backdrop of aesthetically pleasing hardware; Jambox is driven by 'smart data'. By aggregating data from wearables, Jawbone aims to create a contextually relevant picture of individual customers through personal information, biometric data and activity levels. Typically, due to a lack in engagement wearable device users abandon their device after 90 days on average. Jawbone achieves a staggering 81% retention and 20 opens/day which is significantly higher than the industry average. Unlike its competitors, Jawbone has an 'opt-in' model, which empowers consumers to decide which services they wish to benefit from. More importantly, Jawbone does not own any of the information collected through the wearable device. Consumers can choose to delete their data at anytime. The individual app developers have to abide by Jawbone's data deletion clause in order to have consistency across all its service offerings. Hence, they are able to foster an emotional stickiness with their customers through trust and transparency (Merlo, 2013).







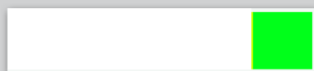

Jawbone Up Privacy vs. Utility Scorecard

Factor	Component	Defintion	Score	Explanation
Privacy (2.8/5)	Quantity	The amount of data collected and saved from wearable devices. This includes: contact details, fitness and health information, in-app behaviour and location. Companies should not collect information that they do not need to deliver valuable communications.	1	Jawbone Up collects and aggregates volunteered information such identity data, biometric data, activity levels, sleep quality and food intake. IT also collects observed data including device type, location and in-app behaviour.
	Transparency	The degree to which a company informs consumers about the information collected and explain the value added to consumers. Privacy policy should be clear and concise to ensure easy consumer reach and education.	4	Clearly stated terms and conditions. Website outlines the data collected and reasons of collection. Although Jawbone claims to gain consent before selling information to 3rd parties. Downloading the 3rd party app implies consent for sharing information.
	Confidentiality	The amount of data that can disclosed without consent of consumer. Information should be used for limited, specifically stated purposes. Privacy policy should include the type of information collected, third parties shared with, reason for sharing and benefits of sharing.	5	Jawbone does not disclose identity data, biometric data, activity levels, sleep quality and food intake to third parties without consent.
	Data Protection	The degree to which information collected is kept safe and secure (Data Protection Act, 1998). There are three components to data protection for wearable devices: Security of operating system, location of data processing and storage and aggregation of data.	2	Jawbone uses its own operating system that uses end-to-end data encryption to ensure safe data transfer from Up to other devices. It uses an open API ecosystem which supports complimentary services. Jawbone also aggregates and processes data in the cloud to better understand consumers. The API ecosystem and aggregation of data makes Jawbone vulnerable to data breaches.
	Salabilty	The act of selling the information collected to 3rd parties. Grading will not only take into considering if consent was taken but also the amount of information sold and the types of companies it was sold to.	2	Jawbone currently does not have a plan for monetising the sale of data for commercial purposes. However, through its open API ecosystem they create a pool of data that is accessible by partner companies who offer premium services.
Utility (4.0)	Functional Value	The second layer of the brand dimensions of differentiation. In includes: fitness tracking, sleep cycle, alarms, durability and design of the wearable device relative to competition.	4	Jawbone offers all expected features, yet the tag price is high relative to competition to reflect the premium brand image.
	Emotional Value	Emotional value is derived from the brand image and communication messages. It includes: Feeling trendy, active or health-conscious person.	3	Jawbone branding is all about making the consumers' life better and creating a community with shared values of health, fitness and an active lifestyle. However, the emotional value is not as powerful as the functional value.
	Augmented Value	The third layer of the brand dimensions of differentiation. It includes delivering unexpected value that differentiates a company in the market. It could includes using perceptive design to deliver targeted and real-time communications.	5	Jawbone is building the first 24-hour contextualised data around consumer to add value and augment the user experience. The purpose of the challenges is to make the users' life better and to create intimacy with the brand. Jawbone also has flexible guarantees which creates goodwill.

(Antabi,2014)

Jawbone Up Gap Analysis and Recommendations

Privacy = 2.8 Utility = 4.0

Target Market	GAP (LITMUS)	Communication Strategy
The Skeptic Privacy = 4.0 Utility = 2.8	Privacy = -1.2  Utility = - 0.2 	The company communications strategy should focus on educating consumers about how Jawbone protects the confidentiality of their personal information. Jawbone does not disclose any identity, biometric, activity level data to third parties without consent. Marketing efforts should highlight this aspect of customer 'opt-in', in order to instill consumer trust. Moreover, the functional benefits of the product should be communicated in order to convince users to adopt earlier. Offline marketing activities such as print, magazines and newspaper may be an appropriate channel of communication given the demographic makeup of the customer segment.
The Rational Privacy = 2.54 Utility = 3.1	Privacy = 0.26  Utility = 0.9 	The company communications strategy should highlight how Jawbone should moves beyond the functional in order to provide a 24-hour contextualised value around the individual. Content marketing should focus on a combination of both case studies and interactive demos, while using competitions and games to connect with customers on a more emotional level (Bosomworth, 2012). These actions may increase relevance and lead to behavioural loyalty.
The Curious Privacy = 1.47 Utility = 3.95	Privacy = 1.33  Utility = 0.05 	Jawbone should focus their communication strategy on how to build an emotional bond with the customer. Since, 'the curious' are intrigued by new experiences, Jawbone have to constantly update its sources of delight by providing unexpected benefits (Merlo, 2013). This may be achieved through updated software features that allow users to do more with their devices. Email and social media marketing may be used to provide interactive demos or links to new features that are soon to be released. By updating sources of delight, the customer will continue to feel engaged with the brand. Hence, increasing customer loyalty.
The Performer Privacy = 0.78 Utility = 4.17	Privacy = 2.02  Utility = - 0.17 	Jawbone should constantly engage with star performers by offering vouchers or discounts for sporting events, concerts and etc. In addition, by providing valuable, relevant and exclusive content this may enhance the level of brand advocacy. The content should be relevant to the Jawbone brand of enhancing users ability to live a better life. Moreover, through crowd-sourcing and online competitions this may lead to higher levels of customer participation and loyalty (Merlo, 2014). Jawbone should provide a platform for users to share their stories with others.