Symantec

SECURITY RESPONSE

How safe is your quantified self?

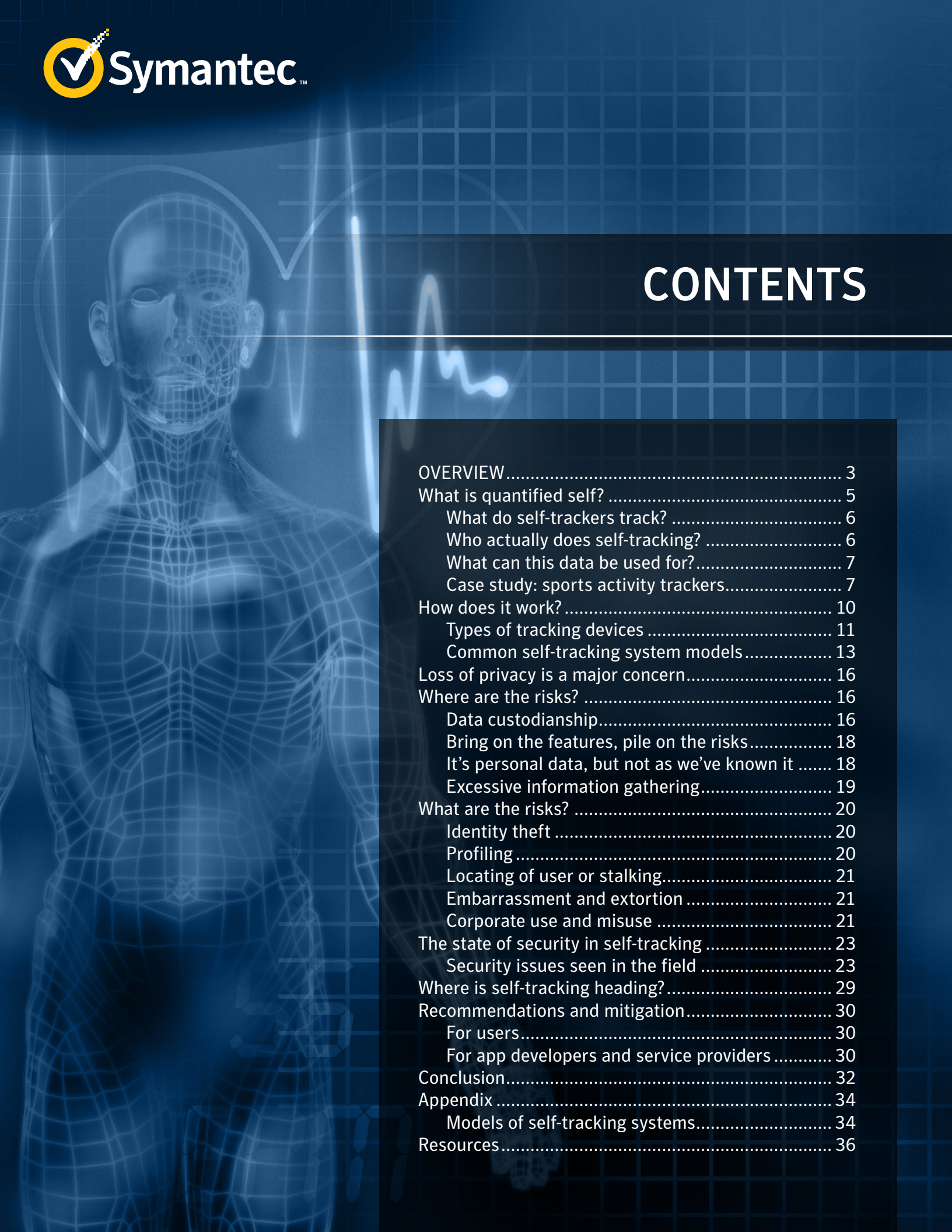
Mario Ballano Barcena,
Candid Wueest,
Hon Lau

Version 1.1 – August 11, 2014, 12:00 GMT

> *Fueled by technological advances and social factors, the quantified self movement has experienced rapid growth.*

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr



CONTENTS

OVERVIEW

Fueled by technological advances and social factors, the quantified self movement has experienced rapid growth. Quantified self, also known as self-tracking, aims to improve lifestyle and achievements by measuring and analyzing key performance data across a range of activities.

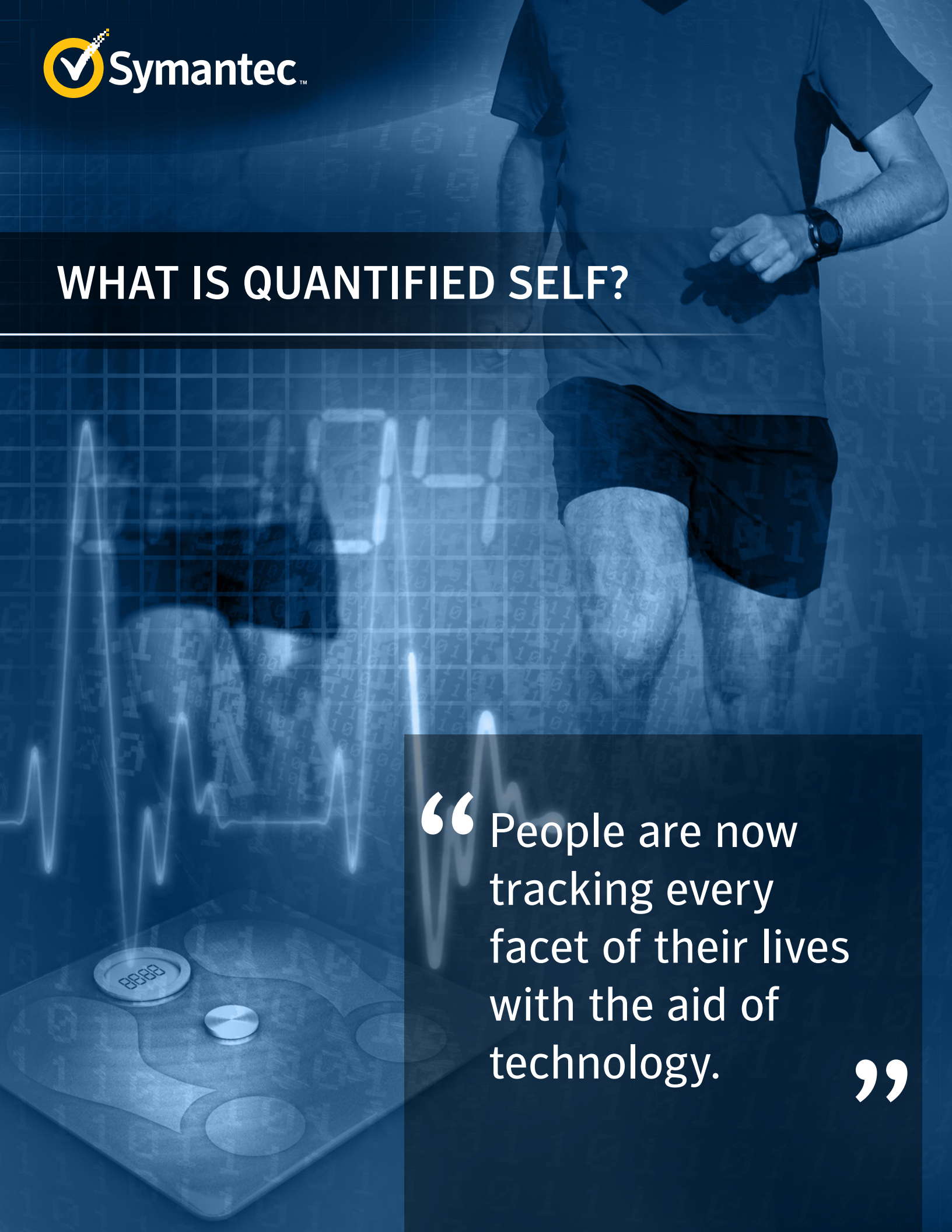
Symantec has found security risks in a large number of self-tracking devices and applications. One of the most significant findings was that all of the wearable activity-tracking devices examined, including those from leading brands, are vulnerable to location tracking.

Our researchers built a number of scanning devices using Raspberry Pi mini computers and, by taking them out to athletic events and busy public spaces, found that it was possible to track individuals.

Symantec also found vulnerabilities in how personal data is stored and managed, such as passwords being transmitted in clear text and poor session management. As we collect, store, and share more data about ourselves, do we ever pause to consider the risks and implications of sharing this additional data?

Symantec

WHAT IS QUANTIFIED SELF?



> “People are now tracking every facet of their lives with the aid of technology.”

What is quantified self?

In recent years the concept of collecting and analyzing data has moved from being mainly used in business to a much more personal level. People are now tracking every facet of their lives with the aid of technology. This, in essence, sums up what the quantified self movement is and what it stands for.

Today, self-tracking is big business and is experiencing rapid growth. A report by ABI Research estimated that the number of wearable computing device shipments will reach 485 million units by 2018. The majority of these devices will have tracking functionality. The number of wearable device shipments only accounts for tracking devices and does not include smartphones that can run self-tracking apps, which would amount to billions. According to a study by the Pew Research Center, 60 percent of Americans now regularly track their weight, diet or exercise activity.

Whatever personal metric a person may choose to track, the goal usually boils down to trying to improve things in some shape or form. You cannot better yourself if you cannot tell if you are better or worse than before. The key to knowing where you are today is to measure and compare against past data, and that is the essence of the quantified self movement.

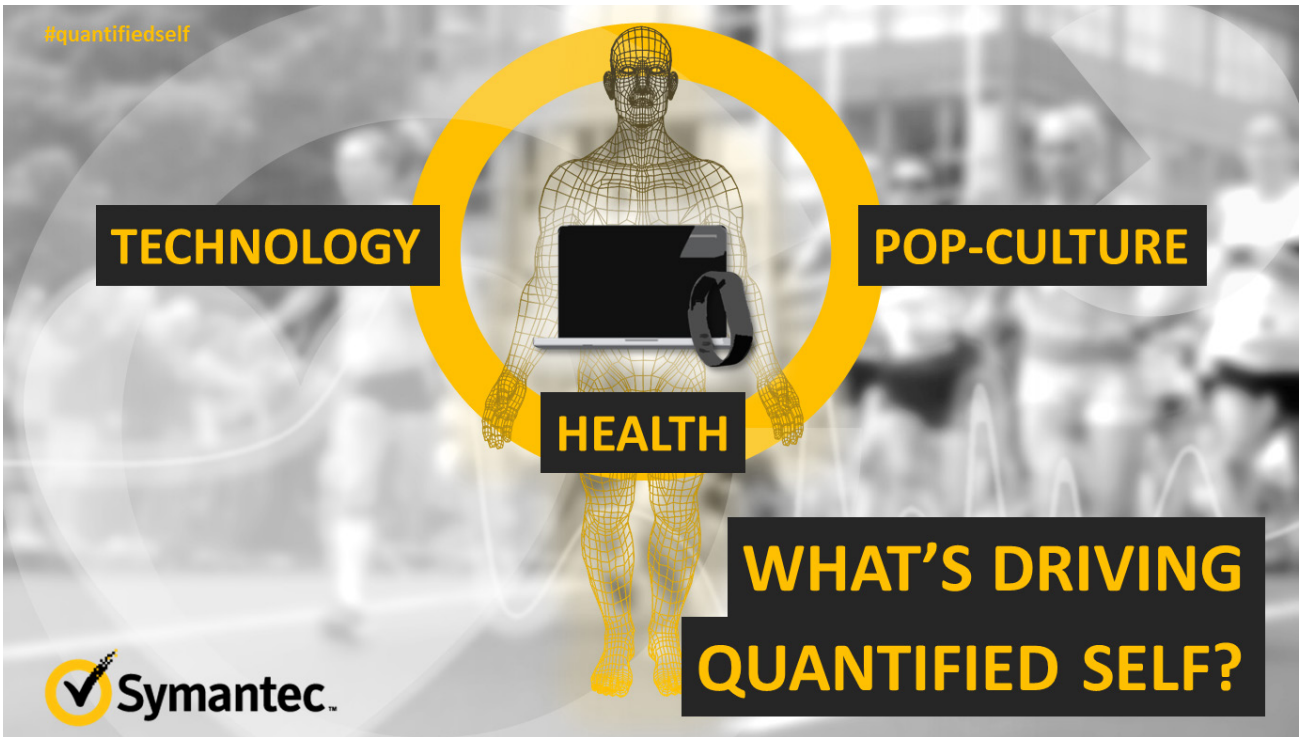


Figure 1. Factors driving growth in quantified self

The quantified self movement is now entering a golden age in its development because of a collision of several forces at play in the world of technology, health, and popular culture. On the technology side, the ever-increasing processing power and miniaturization of sensors and processors, improved battery life, and the rollout of ubiquitous communications infrastructure has opened up a new world of possibilities for always-on devices that can be carried around all day. Another key technology driver is the idea of big data and the wholesale collection of personal data to gain insight into the behavior and habits of consumers.

In health, there is an increasing awareness among the public of healthier living. TV, radio, Internet, and print media publications frequently promote health-related issues, products, services, and lifestyles. After many years of bombardment about health issues, the message may finally be starting to sink in among the general public. On the sociocultural side, there is a trend towards self-awareness, narcissism, and a need to publically express personal opinions and views for social validation. The "selfie culture" and the rampant growth of social networks are classic signs of this trend.

What do self-trackers track?

Today, if you wish to track your activities, you are spoilt for choice when it comes to apps and devices that can help. A quick trawl on the Web reveals that there are apps available to track a multitude of subjects:

Table 1. Examples of types of information that can be tracked using self-tracking apps

Consumption • Calories/food • Alcohol • Nicotine • Caffeine • Water • Drugs/medicine	**Bodily functions** • Body PH • Menstruation/Fertility • Pregnancy • Stool/bowel motion	**Physical activity** • Sports activity • Sleep • Travel • Sexual activity • Tooth brushing
Medical symptoms • Headaches • Pains • Asthma attacks • Allergies	**Spatial** • Location • Altitude • Time • What you see	**Physiological statistics** • Heart rate • Blood sugar/glucose • Temperature • Blood pressure • Weight • Breathing
Mental health • Mood • Stress levels • Alertness		

All that a tracking app or device does is take readings of states from various sensors, then digitizes and stores them for future use. If there is no current or practical sensor technology available to track a certain subject, the infinitely flexible app UI can allow the user to make an assessment of the subject's current state and input data into the app. An example of this is for mood tracking or water consumption.

While much of the information listed is not that sensitive on its own, some of the data could be considered highly sensitive. For example, while medical data requires careful handling, the amount of water you drank yesterday would not generally be considered sensitive information.

Who actually does self-tracking?

Regular practitioners of self-tracking include people with chronic medical conditions who track their symptoms to try and establish patterns in their state, which could help identify correlation factors for their conditions. They may do this as part of a medical care regime or just out of personal interest.

Another common type of self-tracking practitioner is the sports enthusiast. A keen runner could collect data about their running activity to help them set performance goals and track progress. By keeping a log of performance data, a sport enthusiast could determine whether they are improving or not.

Aside from these two types of users, there is a broad swathe of other people who may be just curious or wish to achieve something, such as giving up smoking, losing weight, getting more sleep, or living a generally healthier lifestyle. While the health benefits of many self-tracking devices and apps cannot be scientifically proven, many people clearly believe they are beneficial, as the growth figures in self-tracking apps and devices show.

There are also self-tracking geeks who are interested in documenting all facets of their daily lives in as much detail as possible in public and have turned the whole idea into an art form. Perhaps the most extreme example is Alberto Frigo, who has embarked on an extended journey of discovery to track every detail of his life for 36 years. He aims to record, collect, and photograph a gigantic number of aspects about himself and his environment. His aim is to create a comprehensive record of his life and experiences. Frigo started his journey in 2004 and is currently 10 years into the project. So far, he has recorded a mind-boggling 295,000 photos of things that he has used or interacted with, over 12,000 dreams, over 600 photos of new acquaintances, 7,500

drawings of ideas, and 285 square meters of trash collected from his walks. These are just some of the things that he has collected and recorded so far.

What can this data be used for?

Aside from the clearly stated self-improvement use case, some of this new type of information could also be extremely useful to marketers. Marketing is all about finding out what people want and offering it to them at the right time. Self-tracking data is potentially a goldmine for marketers because it can allow them to gain deep insight into an individual. For example, let's say you like running so you collect and track all of your running activities and upload them to the service provider's cloud servers. By accessing this data, a sports shoe manufacturer's marketing team could learn a lot about your running habits, such as:

- The mileage that you are covering
- When you usually go running
- Where you usually go running
- Where you live
- Your age, sex, height, and weight
- Where and when you are on vacation

Based on this data, marketers could derive valuable insight into your habits and behavior, and could target marketing campaigns to you such as:

- Sending offers for new running shoes when you are nearing the typical shoe replacement mileage (300-500 miles).
- Sending offers for the right type of running shoes. For example, they could offer trail running shoes if the GPS data indicates that most of the user's running activities take place on trails rather than roads.
- Adjusting the price of products and services based on a user's location.
- Sending offers from retail outlets that you often pass by.

All of this knowledge can be inferred either by analyzing data that you typically provide when you sign up or by reading data that is generated during the use of the device or service. However, the really powerful use cases happen when this information is combined with data that has been gathered from other sources. This gives a much more complete picture of the person in question, allowing for far more accurately targeted marketing.

Case study: sports activity trackers

One of the first types of quantified self applications that gained wide user acceptance is the now almost ubiquitous sports activity tracker. This genre of application took off a few years ago when GPS trackers became small enough to be integrated into watches and mobile phones, allowing users to easily carry the trackers around. Using these applications, users can track their sports activity, such as a running session. The tracked data may include start and end times, speed, current location, the route taken, the altitude and so forth. Often, the device that performs the tracking is married to an online service where the data is uploaded. Once uploaded, the data can then be analyzed.

To try and picture the amount of data that could be collected in just one session, let's assume the sports app collects the following data at regular intervals during a session:

- GPS location
- Time
- Heart rate
- Speed
- Altitude
- Steps taken

Data readings are taken at short intervals to provide reasonable accuracy. Suppose the data was sampled once every ten seconds during the session. A one hour running session would generate 360 readings. Suppose the service had one million users and they all used it for an hour every day. That's 3.6 million sets of data generated in one day by just one app. It actually could be quite conservative to assume that a sports tracker app has one million users. A quick scan of a number of popular self-tracking Android apps and services reveal the following download numbers:

- Runkeeper – 10 to 50 million users
- Runtastic – 5 to 10 million users
- MapMyRun – 1 to 5 million users
- Strava Cycling – 1 to 5 million users
- Fitbit – 1 to 5 million users
- Jaw Bone Up – 1 to 5 million users

Based on these numbers, it is clear to see that there is potentially a lot of data being collected, transmitted, and stored on various servers around the world. In today's world, where information is the real currency, these servers are potential goldmines ripe for exploitation. The information could be useful to governments, marketers, businesses, and of course cybercriminals such as the Cyclosa gang who were behind the SSNDOB attacks.

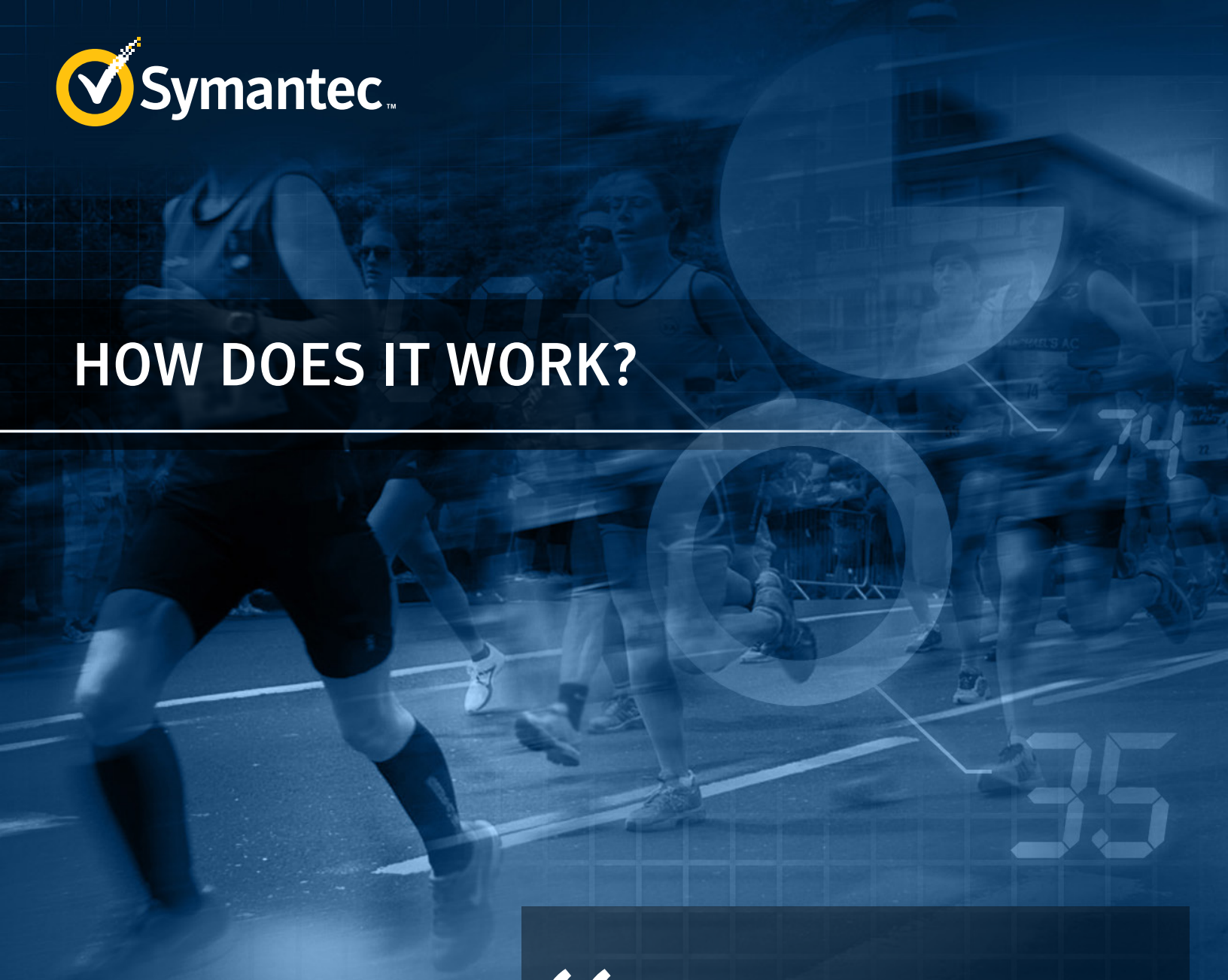
For example, one of the services we looked at states the following key selling points for their device:

- Allow you to discover previously unseen patterns in activity and gain insight into your daily life. (You aren't the only one who might like to know this)
- Track your sleep patterns so you can know when you have the deepest and lightest sleep. (This might be useful for your local burglar to pick a good time to break in)

While the sports tracker usage scenario is relatively benign, there are some instances where leaked self-tracking data could potentially be more damaging or embarrassing if it ended up in the wrong hands.

Symantec

HOW DOES IT WORK?



> “While some die-hards still use pen and paper, most self-tracking today is done using an electronic device.”

How does it work?

Self-tracking is all about turning everyday activities, thoughts, and statuses into discrete data that can be stored, analyzed, and then used to guide a process of change which will hopefully lead to a desired outcome.

The process of self-tracking operates like a cycle and typically works like this.

1. Track and collect data from an activity
2. Analyze and compare performance and status against a desired goal
3. Make adjustments based on findings
4. Repeat process

Figure 2. Quantified self cycle: Track, analyze, and adjust

While some die-hards still use pen and paper, most self-tracking today is done using an electronic device. After data is collected, it needs to be analyzed using software. The knowledge gained from the analysis is then fed back into the process to help guide the user towards a goal. We will now take a closer look at the common classes of self-tracking devices.

Types of tracking devices

There are many ways to self-track activities. An increasing number of people are carrying smartphones and devices with them all day every day, which can be used to collect data. Some tracking devices can also be used to review and analyze data. Devices used in the domain of the quantified self typically come in one of two guises: a smartphone or a wearable device.

Smartphones (with apps)

Most modern smartphones have a plethora of sensors built into them and many of these have self-tracking applications. Smartphones are primarily telephony devices but the inclusion of multiple sensors along with a suitable app execution environment can turn them into general purpose, self-tracking devices. Built-in sensors may include an accelerometer, gyroscope, barometer, heart rate sensor, thermometer, proximity meter, ambient light sensor (light level, usually the camera), and navigation systems such as a digital compass, GPS, and GLONASS.

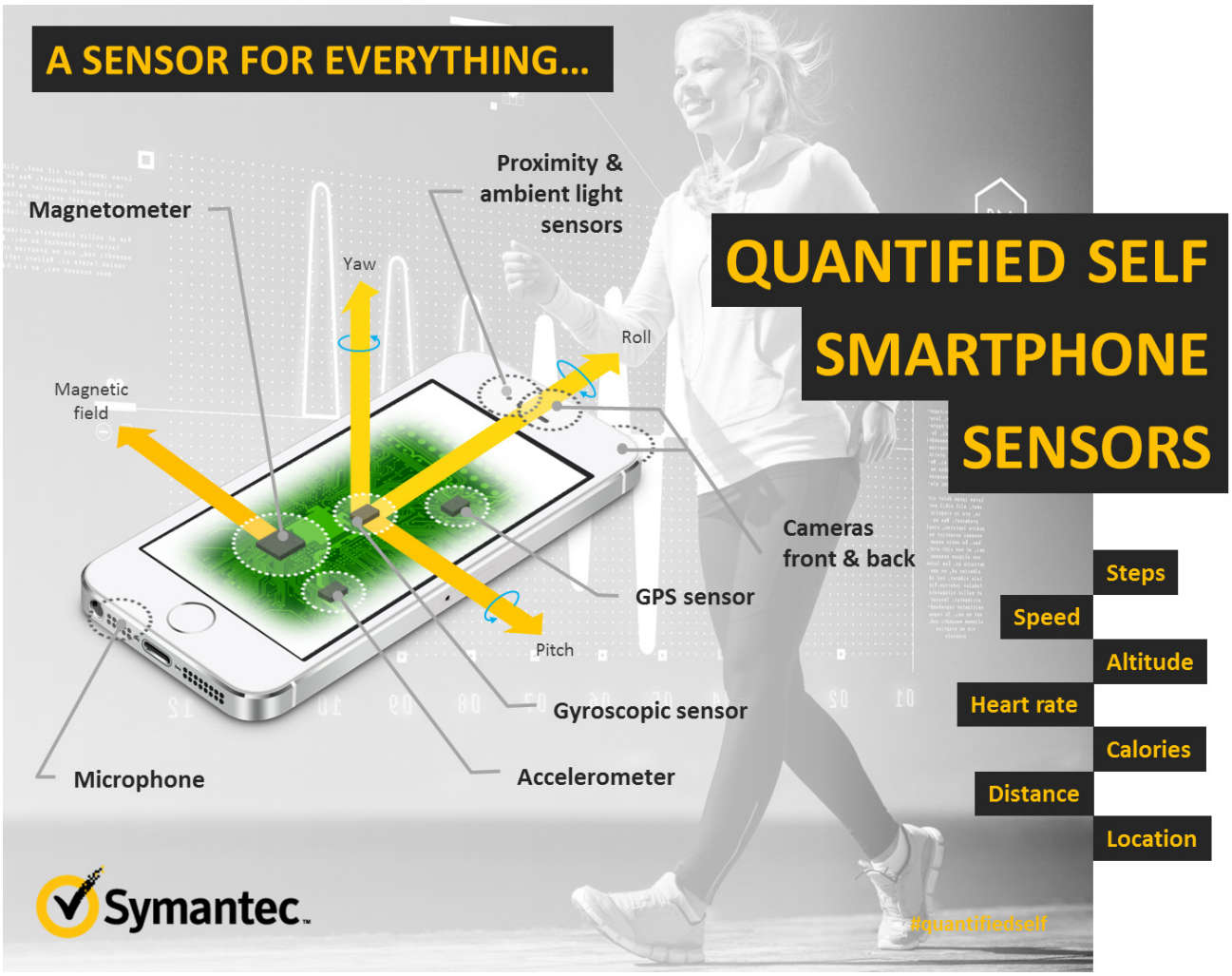


Figure 3. Typical sensors found in modern smartphones that can be used for self-tracking purposes

What these devices actually track depend on the apps the user installs. The app provides the framework to let the device read, store and interpret the signals generated by these sensors. Apps can also let users track data

that sensors cannot currently capture, such as data on moods, food and drink consumption, aches and pains, etc.

Wearable tracking devices

Wearable devices are designed to be worn on the body. These devices typically have a small and light form factor, letting users wear them on the wrist like a wristband or a watch. Alternatively, they can be attached to sports equipment such as running shoes, clothes, bikes, etc. These devices usually contain accelerometers and gyroscopic sensors and these sensors are responsible for generating the data. By reading the stream of data from these sensors and then applying data processing algorithms, the devices can recognize patterns to identify the wearer's current activity.

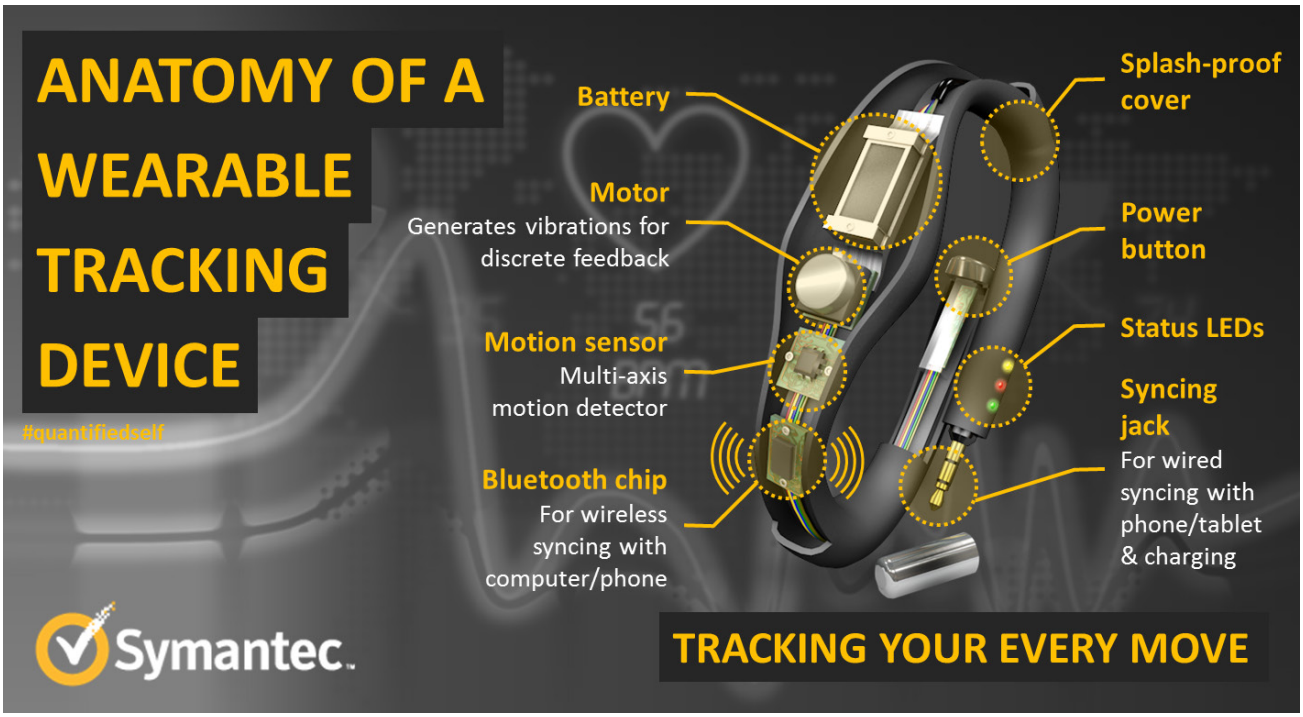


Figure 4. Typical wearable activity-tracking device

Most current wearable tracking devices have a limited user interface, such as a single touch point and a few LEDs indicating the device status or a small dot matrix display. However, this is changing with the increasing number of new smartwatches. Today, the vast majority of wearable devices only perform a data collection function. They require a separate computing device to let the user access data analysis functions.

Common self-tracking system models

Many self-tracking devices, particularly the wearable type, do not have a suitable user interface for analysis and data reviewing. Instead, data must be transferred to another place where it can be aggregated and processed before being presented to the user in an easy-to-understand format.

There are generally three pillars to quantified self systems. Each system may use one, or more commonly, a combination of the pillars to provide an overall service to the user.

Figure 5. Three pillars of quantified self - tracking devices, smartphones and computers, and cloud servers

There are a few general models for self-tracking systems, and they reflect where the processing and storage of data resides. Essentially, data is collected either by a wearable device or a smartphone. The data may then be stored, processed, and presented by the wearable tracking device, the smartphone, or the cloud service, or a combination of the three.

We will now look at two of the most common system models used in quantified self systems. There are other system models used in self-tracking which are detailed in the appendix.

Smartphone app + cloud

Building on the previous system model, in this approach, the smartphone incorporates the required sensors and is used to collect, store, analyze, and present the data. It extends the functionality available locally on the phone by allowing the locally collected data to be synced to the cloud, where additional advanced analytics and services can be offered, possibly at an additional cost by way of a subscription.

This is the most common system model for self-tracking, perhaps for several reasons:

- There is a massive indie app development movement. In general, it is easier to build software apps than hardware. Building hardware requires skills that are harder to find and will require considerably higher investment in terms of money and labor. It is much easier, particularly for smaller companies, to just build software only, rather than building software and hardware.
- There is a large pool of existing smartphones already deployed and

Figure 6. Most smartphone-based self-tracking apps sync with a cloud-based service

actively used. Developers can quickly and easily use the existing rich execution environment and development toolkits to build apps.

- Smartphones already contain many of the required sensors for most self-tracking applications. Since they are already built into the phones and available for use, users do not need to spend more money on extra hardware, making this option more attractive for users.
- Users simply prefer not to carry multiple devices. It is much more convenient to just carry a single compact device that can perform multiple functions than to carry multiple single-function devices. This is true as long as the general purpose device (smartphone) offers a comparable result to specialist hardware. For many functions, this is already the case. For example, a smartphone based app can do an equal or better job of tracking GPS coordinates and monitoring trip performance than many specialist hardware-based solutions.

Figure 7. Examples of smartphone-based quantified self tracking apps that use cloud-based services

Tracking device + smartphone app + cloud

This model is relatively common in systems that use wearable tracking devices. One reason for this may be to reduce costs by leaving out the network adaptor hardware from the device, instead leveraging the one found on the smartphone. Other reasons include keeping the weight and size of the devices down and preventing battery drain. For wearable devices, the size, weight, and battery life are critical factors for its usability and comfort. A wearable tracking device is responsible for providing sensor readings and transmitting the data to the smartphone. Data is typically synced to a smartphone using a wireless mechanism such as Bluetooth Low Energy or ANT+, but sometimes a physical connection may be used. The smartphone app is then periodically synced to the cloud through an Internet connection.

In this model, the smartphone stores some or all of the recorded data, but a copy is also sent to the cloud servers for storage and more detailed analysis as well as other value-adding features. The latter is becoming a more common way for service providers to monetize the collected data by making more detailed or advanced analytics available at an additional price to the user.

Figure 8. Self-tracking system model using a device, smartphone, and cloud-based server

Note: A smartphone in this context could also be a desktop or laptop computer with Internet access.

Loss of privacy is a major concern

According to the results of a survey conducted by Pew Research and the Carnegie Mellon University published in September 2013, 86 percent of adult Internet users in the US occasionally took some steps to try and protect their privacy when online. This figure shows that a significant number of users have an awareness of the risks to their privacy when using the Internet. It also shows that these users are concerned enough about the problem to take some steps to avoid being tracked or monitored when online. Some of the steps taken by users included encrypting communications, using anonymity services such as proxies, Tor, or VPNs, and using a fake name or giving inaccurate information about themselves. The growth of the CryptoParty movement, whose mission is to educate the public on how to use encryption and privacy tools, is a sure sign of a growing public unease about organizations and governments snooping on user's online activities and habits.

Another interesting finding of the survey is that users were most concerned about having their online activities seen by criminals and advertisers. Concern about being monitored by governments was almost at the bottom of the list.

Given this background, it is interesting to note that perhaps the greatest overall risk posed to users by the quantified self movement is the risk of the loss of privacy. Never before has such a huge amount of information been collected, transmitted, and stored about users. People are freely and actively engaging in the collection of information about themselves and, as we will see, the risk to privacy is not improving.

Where are the risks?

When it comes to self-tracking, there are several ways to collect, store, analyze, and present data. Many services involve multipart systems but unfortunately, as more parts are introduced into a system, more risks are added to the equation. Each extra layer in the system increases the risk of attack, as the new elements introduce new potential weaknesses and points of failure which could be exploited by attackers.

Data is generally at risk either at rest or during transmission. What we mean by at rest is when the data is stored for archival purposes such as in a database. Databases can be local, remote, or both. During transmission is when the data is being sent from one device or location to another. Transmission could be performed locally and offline or it could be remotely and online. It can also be done in batch mode or continuously.

Data custodianship

The lifecycle of data handled by most self-tracking systems involve three stages. There is a local data collection phase, a transmission phase, and a cloud-based storage and analysis phase with potential feedback loop. Given this setup, there are three main risk areas for the data collected by self-tracking apps:

- On the device (storage)
- In transit (transmission)
- In the cloud (storage)

On-device risks

Scope of risk: Data about a single user

Data stored on the device is generally about a single user as these devices are usually for personal use. The data stored locally is at risk from malware that can steal data locally. Symantec observed that information stealing is one of the most common traits of mobile malware in 2013, accounting for 28 percent of the threats and 30 percent of mobile malware tracked users. If criminals find valuable data on a device, they are inevitably going to target it. To mitigate this risk, you need proper access control and permissions on the data. The sandboxing

of data is built in to Android and iOS to prevent one app from seeing and interfering with data from another app. This works for the most part, as long as the device is not rooted and no vulnerabilities are found that can circumvent these controls. Encryption of locally stored data should also be considered if the data is considered sensitive enough.

Another obvious risk to locally stored data is the threat posed by the theft of the device. Many self-tracking devices do not offer much in the way of protection in case of physical theft. On smartphones, users can at least make use of the phone locking feature to prevent unauthorized access to data, should the device be stolen.

Transmission risks

Scope of risk: Data about a single user or limited number of users

Data collected by self-tracking apps and devices often need to be sent to the cloud either in real time or in batches, such as at the end of an activity session. Transmission may occur directly from the device to the cloud or from the device, to a computer, and then to the cloud. Indirect syncing may involve the use of short range radio technologies such as Wi-Fi, Bluetooth, or NFC, or cable-based syncing. All of these methods have their own security issues to deal with.

During transmission, data is at risk from an array of possible threats. These include traffic sniffing, which lets attackers collect all transmitted data, and man-in-the-middle and redirection attacks, which could cause data to be sent to the wrong server. One way to mitigate some of these risks is to apply strong encryption and authentication on the data being transmitted. With Wi-Fi, for example, the link could be encrypted with WPAv2. For the local-to-cloud leg of the connection, a network-level security solution such as TLS and a VPN should be used on untrusted networks. Depending on the sensitivity of the data being sent, the data may also be encrypted at the application layer.

Cloud storage risks

Scope of risk: Data about all users

Once data arrives at the cloud destination, it is processed, collated, and stored in a central database of some shape or form. The fact that the database can receive data from remote app clients means it is exposed to the outside world to a lesser or greater extent. This exposure means there is a risk of compromise. Depending on the configuration of the system, there could be any number of risks including SQL injection attacks, account brute-force login attacks, distributed denial-of-service (DDoS) attacks, remote software vulnerability attacks, default password or back door attacks.

The risk in the cloud has a much wider scope. An attacker could break into a single user account or they could compromise the whole system and every user account stored in it by targeting the systems of the service provider or by targeting its staff. Over the years, we have seen countless mega data breaches across a whole variety of industry sectors including healthcare, hospitality, retail, industrial, defense, and government. There is no reason to believe that cybercriminals would be less interested in quantified self data, particularly if it is co-located with other personally identifiable information (PII) such as social security numbers (SSNs) and payment card data.

What can be done? The use of good access controls, strong passwords, and solutions like two-factor authentication (2FA) could help prevent account compromises. Because cloud service providers must expose their service interfaces to the world at large, they are vulnerable to probing and targeted attacks by cybercriminals who wish to gain unauthorized access to the data. Consequently, service providers have a major challenge to ensure that their systems are built and provisioned securely, and are adequately protected on an ongoing basis.

How self-tracking data is managed in the cloud is generally outside of the control or visibility of the users, but they could still get clues as to whether the service providers are handling data in a diligent manner. Users should look for privacy and security statements (for example iCloud, Fitbit, and Jawbone) and compliance with standards such as PCI-DSS, HIPAA, or ISO 27001 where appropriate.

Service providers should at least encrypt all data whether in transit or at rest (you can never be too safe in this age of mega breaches), and there should be appropriate access controls to the data – DLP solutions could help prevent unauthorized access and copying of data. Data should be appropriately segregated too; one user should never be able to access another users' data. Service providers should also consider anonymizing user data as an additional, but not foolproof, layer of security. For example, having a set of GPS coordinates that cannot be linked to a person or time makes the data less useful to attackers.

Bring on the features, pile on the risks

Arguably, the more features and functions that are added to a system, the more complex it becomes and, consequently, the chances of it being less secure increases.

Take, for example, a standalone activity-tracking device with its own data storage and display for showing data. On its own, it does not pose much of a privacy risk. The only risk of anybody else finding out what the owner has been doing is if the attacker managed to gain physical access to the device.

Suppose we add a wireless syncing feature to the device, allowing it to sync to a smartphone app with a better display and more data storage. Syncing in this case is done using Bluetooth Low Energy, a short range wireless communications protocol. By adding this feature, not only have we added more options for usability and functionality, but we have now introduced the risk that an attacker could remotely sniff the data that is being sent over the airwaves. Alternatively, attackers could undermine the wireless device syncing mechanism by trying to hack into it through security weaknesses or by forcing or tricking the device to connect with a computer controlled by the attacker.

Even if data is synced by wire, merely storing the tracking data on another device increases the risk profile, because now the data is stored in two places. In many cases, the device where the data is synced to tends to hold both personal and aggregate data. The volume of data is much greater and increases the potential impact if an attacker compromises the data.

Suppose we now extend the functionality further by adding online cloud service functionality. After a user has synced their data to the smartphone app (which is still within the user's physical domain), they now have the option of uploading their data to an online cloud service for safekeeping, analysis, and social sharing. Add social media integration and an API to allow third party developers to build apps that leverage the data and the risks mount up.

Unlike data in the user's domain, the cloud service domain is mostly outside of the users' control. Users have limited control over authentication, authorization, access, and sharing. Almost everything else, including the responsibility for control and security, is handed over to the service provider who chooses how to protect the data, how it will use the data, and who it will share the data with.

With the addition of a cloud service layer into the system, suddenly the attack surface is much larger and more difficult to defend. The risk of attacks can now come from remote locations and attackers can attempt to intercept network traffic to steal data from individual users or target the mother lode by attacking the cloud service provider directly. A successful compromise of a cloud service provider, allowing access to the user database, could compromise all of the users of the service.

It's personal data, but not as we've known it

Over the years, many of us have grown accustomed to sharing a certain level of information with online service providers. For example, many services request a full name, date of birth, phone number, address, email address, password, and security questions and answers when the user signs up. Most of us have come to accept this as a trade-off for using the services. Some information, such as the IP address, may also be involuntarily collected and recorded without any user intervention.

The risk to privacy increases considerably as the amount and range of data known about us increases. When it comes to risk, everything depends on the context. A single piece of personal information on its own, such as a date of birth, provides no context and poses few risks to anybody. Thousands of users in a website database

could share the same date of birth, so that information on its own does not allow any one person to be singled out. However, if we can associate a first and last name to the date of birth, suddenly the number of matching users in a database may shrink dramatically.

When we talk of "personal information," names, contact details, and dates of birth are the type of information that we typically think of. We could call this traditional personally identifiable information (TPII). But now, new technologies enable us to collect much more information at a deeper and more personal level. Data generated by self-tracking devices and services (also known as first-party data) is potentially highly personal and could reveal an awful lot more about ourselves to others than we may like.

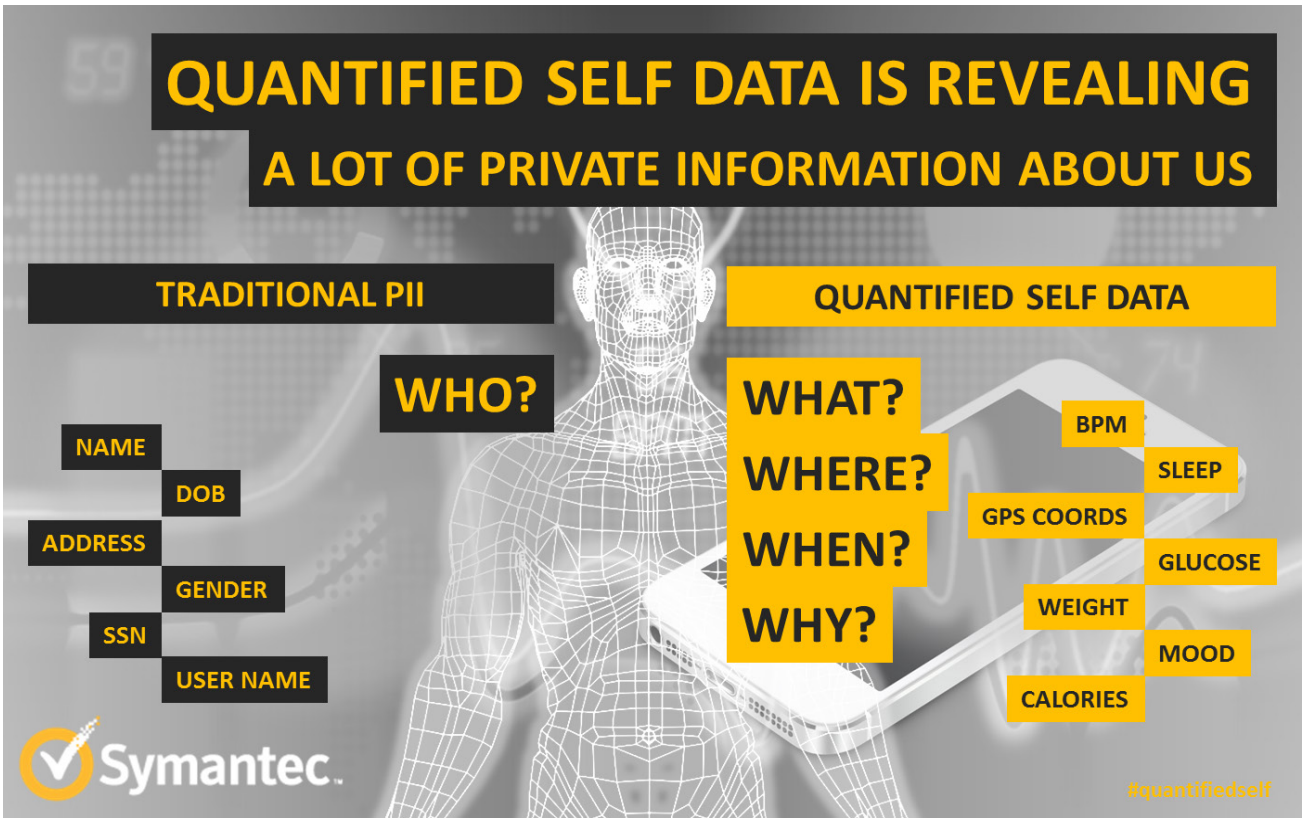


Figure 9. Traditional PII versus self-tracking information - tells a different story

Traditional PII can tell somebody about who we are, where we live, and how to contact us. Additional information generated by self-tracking services can tell somebody about what we do, where we are or have been, and when and potentially why we are doing something. When additional self-tracking information is combined with traditional PII, the potential for abuse becomes even greater. As more data is aggregated and relationships between data are formed, data becomes information and, after further analysis, becomes insight which can be used to predict the future behavior of people. This is gold dust to marketers as well as cybercriminals.

Excessive information gathering

While it is understandable that some self-tracking services need to know certain personal information in order to provide a useful service, some services ask for a lot more information than is really necessary. For example, it would be reasonable to expect a sports activity tracking app to ask for the user's age, gender, weight, and height in order to calculate certain statistics such as the estimated calories burnt during an exercise routine. However, would such a service need to know the user's home address, relationship status, education, or work background? Would these factors have any bearing or impact on the user's fitness or the provision of the service to an

individual? Some of these data points are more appropriate for a consumer survey so before signing up, users need to ask themselves whether they are signing up for a service or a marketing survey.

There's a saying that goes "If You're Not Paying For It, You Become The Product." Many online services offer their products for free but these are businesses and they have to generate revenue to survive. Instead of making users pay upfront, they use revenue generation strategies such as advertising and collecting and selling marketing information. This is a trade-off that users need to be aware of when using online services.

The next time you are asked for your date of birth, ask yourself whether the date of birth is really needed or if a year of birth would suffice.

Thankfully, a lot of this extra information gathering is optional, but users should be aware of what is a reasonable amount of information required to effectively operate a service compared to unnecessary and excessive information gathering.

What are the risks?

The following are some of the things that your private self-tracking data could potentially be used for:

Identity theft

There is a criminal industry that prospers on gathering and selling as much PII as they can get their hands on. Complete sets of data about a person can then be sold to other criminals in packages known as "fullz." In this criminal business, the more complete and up to date the set of details is, the more valuable it is. Having a more complete set of data about a person can allow fraudsters to better fake official documents or commit other frauds. For example, details could be used to set up false bank accounts for money laundering, ransom attempts, or IRS fraud through fraudulent tax returns.

The threat of data theft or misuse does not have to emanate from outside of an organization. There have been many incidents in the past of rogue employees selling customer information to third parties for personal gain. These range from small scale incidents to massive data theft incidents involving millions of users.

Profiling

Many organizations already use profiling to target, exclude, or even discriminate against certain types of people based on personal information that they have collected about them. Details provided by users to self-tracking services could enable marketers and government agencies to organize and target certain types of users. Profiling is of concern to privacy and human rights advocates because it can be easily misused to the disadvantage of certain groups or minorities.

Insurance is likely to be one of the key beneficiaries of self-tracking data. There is already much discussion about how insurance could use quantified self data. We are already seeing some limited use of self-tracking data for insurance applications where some employers are using it to discount health insurance policy premiums based on certain perceived positive behaviors such as leading a healthy lifestyle.

In usage-based or telematics insurance, tracking devices (which can be considered as self-tracking devices) are fitted to cars to track the driving habits and performance of drivers in return for reduced insurance premiums. More time on the road combined with bad driving habits such as hard acceleration, late braking, and fast cornering - behaviors that fit the profile of aggressive driving - may result not only in an increased fuel bill and added wear and tear to the car but insurance premiums will likely increase too.

Locating of user or stalking

Location-based self-tracking PII could also be abused for criminal purposes if it was to fall into the wrong hands. For example, if criminals were to gain access to a sports tracking database, they could determine where a person lived and when they would be most likely to be away from home and plan a break-in accordingly. Over the years, there have been stories of people having their homes broken into while on vacation due to social media postings of pictures and updates showing that they were away from home. You could obtain this kind of information from many self-tracking service cloud databases.

Accurate and real-time location-based tracking can be useful for some activities, but this information could also be useful for stalkers and even private investigators and governments who can use this information to locate their targets.

In some countries, the police can use average speed detection systems to catch speeding drivers. These systems work by capturing the time and license plate of a car as it enters a road segment and then again when the car leaves the area and works out the average speed to cover the distance between the points. This system would not be necessary if everybody had tracking devices in their cars and the police had access to monitor the location and movements of all vehicles in real time, but the privacy implications of this level of mass surveillance might be too much for it to ever come to pass.

These are just some of the risks that can arise from having your location tracked and exposed. There are countless other scenarios where you may not want your location to be known.

Embarrassment and extortion

We have already seen that self-tracking services can track much more than just fitness and sports performance. There are many services that track medical or health related activities and bodily functions. For example there are self-tracking applications that can track the mood, toilet, and sexual activity of users. Are these the types of data that we would be happy to share about ourselves? Does anybody but yourself, or perhaps your doctor, need to know when the last time you went to the toilet was? Would you be comfortable with the exposure of this type of information about yourself to the world? Perhaps a person who suspects that their partner may be cheating might be interested in data collected from these devices.

We have already seen many cases of sensitive information (intimate photos or videos for example) falling into the wrong hands and then being used to extort money from victims. As more and more sensitive information is collected and transmitted around the world, the risk of highly sensitive data falling into the wrong hands increases.

Corporate use and misuse

Self-tracking service providers have not been slow to catch on to other potential business applications for data generated by self-tracking technologies. Some vendors in activity tracking technology actively promote the use of their devices in corporate wellness programs. The benefits touted may include cheaper health insurance, decreased sick leave, decreased healthcare costs, and even increased productivity due to employees feeling more positive as a result of a more active lifestyle promoted by use of these types of devices.

Not all corporate uses garner a positive reaction. A supermarket chain in the UK uses tracking devices to monitor the activities of staff to help improve work efficiency. The staff members who are required to use these devices have expressed mixed views about them, with some saying that these devices are putting staff under immense pressure to perform.

Despite many businesses' best intentions to keep customer information safe, their databases are often the target of cybercriminals who attempt to break in and steal the information. There are also insider threats to businesses and there have been many stories in the past of employees of businesses stealing customer information and passing it on to various agencies for a fee. Insiders can pose a considerable threat as staff may have privileged access to data, making it easier for them to copy or manipulate it.

Symantec

THE STATE OF SECURITY IN SELF-TRACKING

> “Users of wearable self-tracking devices can be tracked remotely without them realizing.”

The state of security in self-tracking

Self-tracking apps and services are essentially just another category of apps that run on mobile devices. What is common about them all is that they are designed to record information about the person. Because these services are just another type of mobile app, it should come as no surprise that they share many of the same kind of security issues that have been seen in other mobile apps.

For research purposes, we examined a range of popular self-tracking devices and mobile phone-based health and fitness apps to see what kind of security issues we could find.

Security issues seen in the field

Granular location and personal tracking

KEY FINDING: All of the wearable activity tracking devices examined, including those from leading brands, are vulnerable to location tracking.

This is tracking the location of a person to a high level of granularity and detail. In some self-tracking applications, there is a necessary and expected trade-off between privacy and functionality. This scenario typically applies to GPS-based activity trackers such as smartphone sports tracker apps or GPS-based self-tracking devices like sports watches. People use these devices and services knowing full well that they will be tracked and are happy to do so because they choose to have their location tracked during the session.

What is more problematic is when users are tracked without knowing they are being tracked or can be tracked. This can arise even when people are using devices that have no obvious means for location tracking.

Most self-tracking devices are simple in their makeup. They typically contain a few physical sensors such as accelerometers, gyroscopic sensors, and tilt meters. These are used to detect patterns of motion that are then

Figure 10. Many Bluetooth-enabled devices can be easily tracked

interpreted as certain activities. In our research, we found that all of the devices we looked at either had a USB and/or a Bluetooth interface, most commonly Bluetooth Low Energy (aka Bluetooth Smart). The latter option allows the self-tracking device to be connected part-time or continuously to another computing device without wires, which makes it very convenient for users as well as those who want to track them. As it turns out, many of the current activity-tracking devices on the market, such as the sports wristbands or pendants, can be easily tracked.

The key to how these seemingly offline devices can be tracked comes down to how they use the Bluetooth LE technology. Many Bluetooth LE devices are assigned a specific hardware address, much like the way standard computer network cards have a fixed MAC address. When in use, Bluetooth LE-enabled devices can transmit a short range (<100m) signal that advertises itself to nearby devices. This signal can be read by anyone within range and, depending on the device, it may contain information necessary for a connection to be established. This information also includes the fixed Bluetooth LE network address. In some cases, the devices may also expose other information that could be used for tracking the device. The information may include serial numbers or other internal IDs specific to the device and could be accessed simply by performing a remote querying operation on the device.

By placing a number of scanning devices at various locations, it is possible to scan and locate a device. By identifying the hardware address and measuring the relative signal strengths between scanners and the device, it is possible to get an approximate fix on the physical location of the device.

For this project, we built a number of Bluetooth scanning devices using Raspberry Pi mini computers coupled with a battery pack, an SD card and Bluetooth adapter, for the low price of US$75 each. (We call them Blueberry Pi!) We placed them at selected points along the course of a major European running event to see what we would find. When we looked at the data, we found that some of the runners were self-tracking devices that could be tracked using Bluetooth scanners. By placing scanners at various points of the race, we could determine when a

Figure 11. One of our Blueberry Pi scanning devices

device passed the scanners and, by comparing times when the device was picked up by different scanners, work out the average speed of the competitor.

We also performed a similar scanning exercise by walking through the busy city center streets of Dublin, the capital of Ireland, and also at public transport hubs in Zurich, Switzerland. During these separate scans, we also picked up a range of self-tracking devices and a large number of mobile phones and tablet devices. These simple scan results show that it is relatively easy for these devices and, by extension, their owners to be tracked.

The scans also showed that there are quite a few people wearing these devices when going about their business around the city. Interestingly, during our scans, we found that one vendor for self-tracking devices dominated the marketplace, with three quarters of devices found coming from this one vendor.

Tracking problems are not limited to Bluetooth LE devices. The problem has been well documented in Wi-Fi. Currently, as you walk around with Wi-Fi enabled on your portable device , your device is giving away its unique MAC address, which means it is possible for somebody to track your device (and℠ by extension – you) from afar. In recognition of this issue, Apple recently announced that one of the changes to be included in iOS 8 is the use of randomized network IDs when the phone is scanning for Wi-Fi access points. Only when the user chooses to connect with a found Wi-Fi network will the true MAC address be revealed. This shows that major vendors have recognized that network address tracking and its privacy implications are a real threat to users.

Transmission of tracking and personal data in clear text

KEY FINDING: 20 percent of apps transmitted passwords in the clear

Most of the self-tracking services that we looked at required or offered online cloud-based service components for which users have to create an account for in order to use. Whenever there are user accounts, user names and passwords are never far away so we were interested to see how the different services handled sensitive information such as login credentials. We were disappointed to find that out of all the apps that we looked at that required user logins, 20 percent of them transmitted user login credentials in clear text, meaning no attempt is made to encrypt the passwords at all. In a couple of cases, unsalted MD5 hashes of the passwords were sent, perhaps as a way of securing the passwords, but unsalted MD5 hashes are easily crackable with rainbow tables so this offers little protection. In some cases, due to deficiencies in the design, a cybercriminal could just use the password hash itself (no need to crack the hash) to log into an app, as the hashing of the submitted password is performed in the app (client side).

What is particularly worrying about this finding is that there is already ample evidence available to show that many people reuse the same user name and password for multiple services. It only takes the weakest link in the chain to expose credentials which could then be used by attackers to take over other accounts that have a more secure setup.

In other cases, self-tracking and other personal data may also be transmitted without the use of a secure channel. Transmission of data in clear text leaves the user data wide open to data sniffing. The classic example is when users are connected to unsecure Wi-Fi networks to transmit data. A number of apps that we looked at exposed the email address and other account data as well as details of the user's activities in this way. Given that so many of the apps transmitted login credentials in clear text, it does make us wonder how the data that is stored on the server side of these services is treated. We have seen plenty of cases of server data breaches where user names and passwords were stored in plain text in databases. The bottom line is user credentials and data should always be encrypted at rest and during transmission and vendors need to ensure that they handle sensitive data appropriately.

Lack of privacy policies

KEY FINDING: 52 percent of apps examined did not make available privacy policies

Self-tracking apps and services are by their nature designed to collect and analyze personal information. Therefore it is reasonable to expect and indeed is legally required (such as in the Online Privacy Protection Act 2003) of companies that collect and manage PII to make a privacy policy available that is displayed prominently and easily accessible. Privacy policies should preferably be understandable even by those not in the legal profession and must be shown to users before they sign up for a service so that they can make a considered choice before using it. The policies should typically explain to the user the following:

- Who is collecting the data?
- What is being collected?
- When is data collected?
- What will the data be used for?
- How long will the data be kept?
- How can the user access and control the data?
- Will the data be shared with third parties?

Privacy policies are important because they form part of the user contract. While privacy legislation may vary from country to country, in general, information that is collected may only be used for the originally stated purpose.

Despite the importance of having a privacy policy, the majority of apps did not have one. Of the other 48 percent that did have privacy policies, many of them used generic privacy statements with vague promises of keeping user data private without any elaboration. The lack of a privacy policy may be a possible indicator of how the issue of security is treated in the development and provision of online self-tracking services. Users would be well advised to take this into consideration before signing up for any services.

Contacting multiple domains

KEY FINDING: The maximum number of unique domains contacted by a single app was 14

The average number of unique domains contacted by the self-tracking apps that we looked at was five and the maximum number was 14. While it is understandable that apps may need to contact a few domains in order to transmit collected data and access certain APIs such as for ads, it come as a bit of a surprise that a significant number of apps contacted 10 or more different domains. The types of domains contacted can be categorized into the following areas:

- Service provider (to transmit user data)
- OS provider
- Ad networks (Tapjoy, Doubleclick, Amobee, Simpli.fi)
- CRM/Marketing services (Apsalar, Localytics, Apptentive, Flurry, Admob, Appsflyer, Aro, Uservoice, BudURL, Mixpanel, Adjust, Kiip, Urbanairship, Fiksu, Google Analytics)
- App analytics and testing (Crashlytics, Crittercism, Testflightapp, Bugsense, Newrelic,)
- Social media APIs
- Utility API (Forecast, Wunderground, Appspot, Mapping services)
- App frameworks (Parse, Amazon Web Services, Appspot)

While the apps may have legitimate business reasons for contacting many different domains, from a user's perspective, many of the domains being contacted are receiving information on the user's behavior and activities (metadata) without the user actually being explicitly informed about it. In some cases, a reference may be made in a privacy policy but in general, metadata collection appears to be considered as fair game. Therefore, it is not surprising to find that many of the third-party domains being contacted belong to CRM/analytics and marketing services. These services allow the app provider to monitor and track user behavior in relation to how users use the app and respond to different offers and features. It is great for the app developers because it allows them to conduct user research and gain insight into user behavior, but it is not so great for using the users' data plan

allowances and their privacy. This point neatly leads us onto the next issue of unintentional data leakage.

Weak session management and security

With user account-based services, one of the dangers is that session management in the service may be insecure. Weaknesses in this area may enable attackers to guess user accounts in the system and then hijack sessions or access data belonging to other users in the system. One of the simplest ways to do this is to guess or even simply increment the session or user ID while logged in with a valid session of another user. Poorly designed systems will permit this to happen and reveal data from other users. In our study, we found a number of apps that showed this type of weakness. One particular system was so poorly designed that it could expose user accounts data if you know the email address of one the users of the system or if you simply modified the user ID in the request as the IDs are sequential.

Session IDs should be large alphanumeric strings that are randomly generated by cryptographically safe methods and should only be valid for one given user ID. Clearly some vendors are falling well short of the mark.

In one case, we found a particular app that exchanged whole SQL statements with the server to create new tables and update them. This type of setup could open up a huge security hole that can be exploited by attackers to gain unauthorized access or manipulate the database by modifying queries sent by the app.

Unintentional data leakage

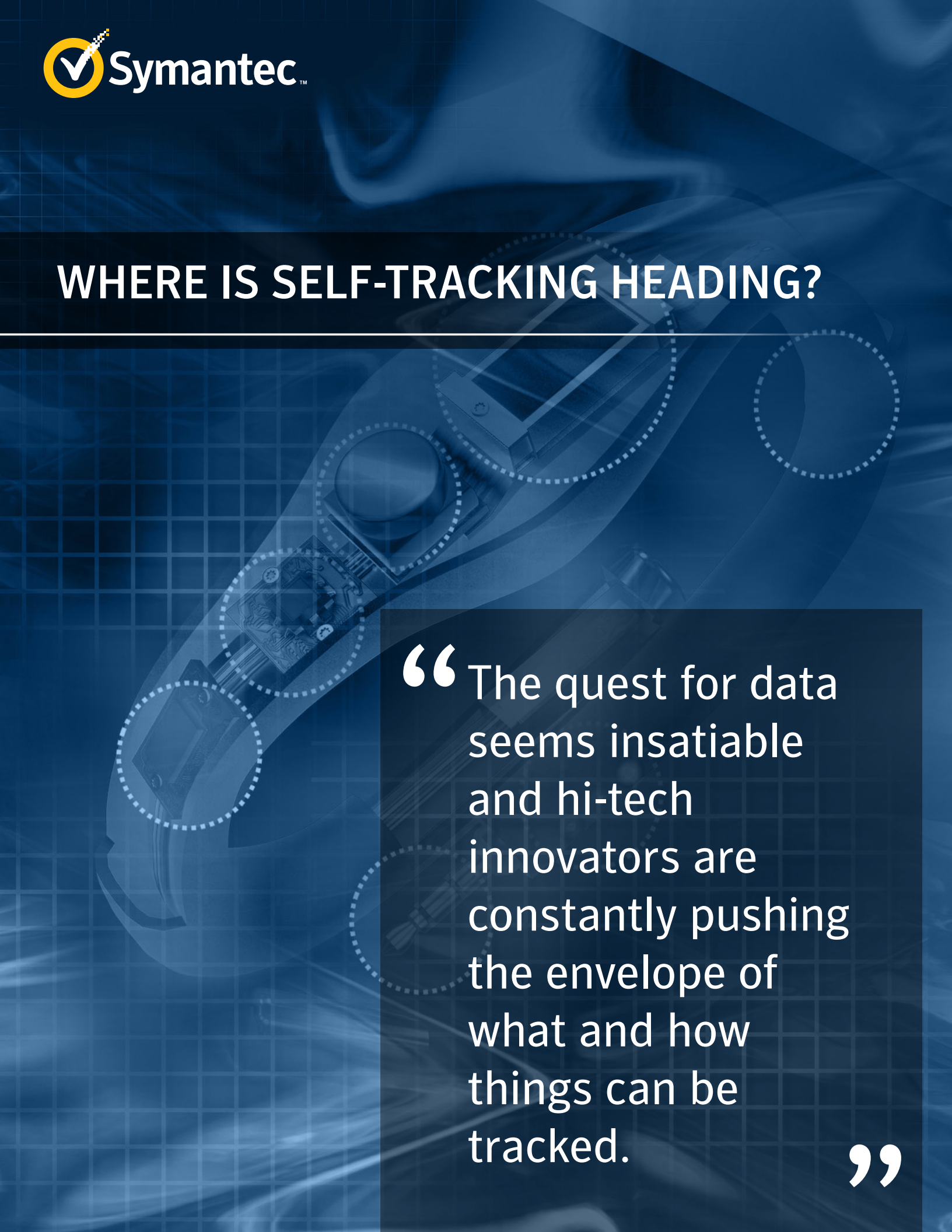
Despite the best intentions of app developers, information about users' activities could still be revealed in the most unlikely of ways. For example in one app that tracks sexual activity, the app makes specific requests to a certain analytics service URL at the start and end of each session. In its communication, the app passes a unique ID for the app instance and the app name itself as well as messages indicating start and stop of the tracked activity.

Based on this information, the third party who receives the data would be able to know the sexual habits of the owner of the device, granted that the real identity of the device owner may not be associated with the ID. In this case, the network exchanges were being made to request ads which will then be displayed to the user whenever they are finished doing what they are doing. Because the requests for the ads are made in a deterministic way whenever the activity is completed, it is possible for a third party to infer what the user has been doing. In addition, the app also sends start and end messages to an analytics service provider which could enable a person with access to the analytics data to determine the activities and performance of users of the app. Despite the makers of the app promising that none of the users' data is ever transmitted over the Internet, some of the users' activity can still be leaked through the network behavior of the app.

Aside from the scenario mention previously, there are also countless other scenarios where personal data could be leaked unintentionally such as through human error or social engineering or just shoddy handling of data.

Symantec

WHERE IS SELF-TRACKING HEADING?



> “The quest for data seems insatiable and hi-tech innovators are constantly pushing the envelope of what and how things can be tracked.”

Where is self-tracking heading?

Despite the security challenges in self-tracking, public interest in it has mushroomed in the past few years and there is no shortage of new startups and big players jumping into this space. One indicator of this interest is in the amount of startup activity in this line of business. According to CB Insights, funding for quantified self-related startups reached US$318 million in 2013, that's up 165 percent from 2012. According to a report by app analytics firm Flurry, the first six months of 2014 saw a 62 percent growth in the use of health and fitness apps. Clearly this market segment is still in the rapid growth phase.

Another good indicator of where the market is heading can be had by observing what the major hi-tech giants have been doing in this area. Many of them are making significant moves into this space. Facebook purchased ProtoGeo, the maker of Moves in April 2014 for an undisclosed sum. Before the deal, Facebook already had one of the most comprehensive and detailed databases of users, encompassing everything such as who their friends and contacts are, what the user likes or dislikes, where they are going or have been, as well as their relationship status and photos. By purchasing Moves, the social network adds detailed self tracking information to its collection which gives it an unrivalled view into the lives of users.

Not to be left out of the picture, both Apple (HealthKit) and Google (Google Fit) have also announced major forthcoming initiatives aimed at helping health and fitness category app builders tackle the challenges of developing these types of apps. These initiatives will undoubtedly help to feed the growth in the health and fitness category of the app market.

There will also be increasing crossover between wearable technology, the quantified self, and the Internet-of-Things. As a result, the quantified self is increasingly morphing into something that is more akin to quantified things, that is, the tracking of things owned by a person. Take for example Whistle – a tracking collar for your dog or the quantified dairy cow using Lely T4C InHerd.

The quest for data seems insatiable and hi-tech innovators are constantly pushing the envelope of what and how things can be tracked. Recent developments such as the MindRDR app for Google Glass sshow that we are not too far away from being able to achieve the ultimate in life-logging and self-tracking — the reading and logging of our own thoughts.

In recognition of the relentless trend towards collecting and using personal data by businesses, some individuals are attempting to trigger a counter movement to regain the initiative in favor of the user or data subject. Take for example the citizenme project founded by St John Deakins, which is created in an attempt to redress the balance of power between those who are collecting and selling our data and ourselves, the data subjects.

Recommendations and mitigation

Both users and service vendors have a role to play in ensuring self-tracking security.

For users

The following steps could help users stay safe when using self-tracking apps:

- Use a screen lock or password to prevent unauthorized access to your device
- Do not reuse the same user name and password between different sites
- Use strong passwords
- Turn off Bluetooth when not required
- Be wary of sites and services asking for unnecessary or excessive information
- Be careful when using social sharing features
- Avoid sharing location details on social media
- Avoid apps and services that do not prominently display a privacy policy
- Read and understand the privacy policy
- Install app and OS updates when available
- Use a device based security solution
- Use full device encryption if available

For app developers and service providers

App and service providers should observe the following points to help provide a secure experience for users:

- Build security in from the start, not as an afterthought
- Always use secure protocols when transmitting data
- Ensure that the device is not directly or indirectly traceable
- Only collect data that is necessary to provide a service and nothing more
- Require strong passwords for user accounts
- Implement secure session management
- Follow best practices for password handling (only store salted hashes and not the real password)
- Follow secure coding practices
- Provide an easy to understand privacy policy and act within the stated policy
- Pen test system infrastructure to ensure security
- Ensure that backend systems are well protected from intrusion
- Make security testing a part of the product development process
- Ensure that staff are properly trained on how to handle sensitive information
- As a data controller, be sure to comply with relevant data protection laws

Symantec

CONCLUSION

> “The self-tracking craze is causing an explosion of personal data to be generated, transmitted, and stored about ourselves.”

Conclusion

The self-tracking craze is causing an explosion of personal data to be generated, transmitted, and stored about ourselves. Ultimately, the more data that we collect and store about ourselves, the more opportunity there is for us to learn about ourselves, but it also opens up the opportunity for others to learn the same about us.

In this paper, we have examined some of the issues that can arise from the relentless rush to generate data about ourselves. We have examined the types of self-tracking systems that are currently in use today and how they generate and handle data. We have looked at the current state of security in the self-tracking space and found it to be lacking in some key areas. For example many apps and services lacked privacy policies and disturbingly, even basics such as the secure handling of user names and passwords are not done correctly by a significant number of apps.

We also found that even devices that are not obviously traceable can still be tracked wirelessly due to implementations that do not to use available privacy features.

With cloud-enabled systems, the user passes over much of the control and responsibility for safekeeping to the cloud service provider who takes over custodianship of the data. The data held at the cloud service level has a much wider scope of content and aggregates the data from all users of the app. The database could contain data for millions of users and their activities. This places an onus on cloud service providers to ensure that they implement the appropriate level of security and best practices to safeguard data integrity and privacy. Sadly, as we have found in our research, the required level of care is not always taken, leaving users at risk. Service providers should strive to ensure that security is at the core of the service from the device all the way to the cloud. Security should be at the forefront rather than merely an afterthought.

So far, we have not seen large numbers of significant data breaches against operators in the health and fitness app category but there has been some. As the sector continues to experience rapid growth, we can expect that it will soon begin to register more prominently on cybercriminals' radar and the question about possible data breaches against major players in the health and fitness app sector is going to be about when, and not if, a breach will occur.

Having scratched the surface of this burgeoning sector and glimpsed inside, we would conclude that there are positive signs that some vendors are doing the right things, but far too many are not. Just how safe is your quantified self? We think that it could be an awful lot safer than it currently is, so before you install the next new self-tracking app on your smartphone or buy that new self-tracking device, pause for a moment and think before you track.

Symantec™

APPENDIX

Appendix

Models of self-tracking systems

The following are the most commonly used system models among self-tracking systems. The following table summarizes the risk levels and various points at which data is collected, transferred, analyzed, and presented in each of the common system models used.

Table 2. Table of self-tracking system models

System model	Privacy risk	Data collection point	Data storage	Data transfer mechanism	Data analysis	Data presentation
Tracking device	Low	Device	Device	None	Device	Device
Tracking device + smartphone app	Medium	Device	Device Smartphone	WiredWireless	Smartphone	Smartphone
Tracking device + cloud	Medium	Device	Device Cloud server	WiredWireless	Cloud server	Cloud server
Tracking device + smartphone app + cloud	High	Device	Device Smartphone-Cloud server	WiredWireless	Smartphone-Cloud server	Cloud server
Smartphone app	Low	Smartphone	Smartphone	None	Smartphone	Smartphone
Smartphone app + cloud	High	Smartphone	Smartphone-Cloud server	Wireless	Smartphone-Cloud server	Cloud server

Tracking device only

In this model, the data is collected by the tracking device and the data stays on the device. The device fully handles processing and displaying the data. There are not many modern self-tracking devices that operate in this way. For example, old style pedometers work in this way. They are typically not connected in any way and the data stored within them is private and not shared with any third parties who do not have physical access to the device. The limited display is used to show all of the data and statistics captured.

Figure 12. Example of a basic wearable tracking device, a pedometer

Tracking device + smartphone app

In this model, the data is collected using a wearable tracking device. The data is then transferred to an app that runs on the smartphone. The app is then responsible for aggregating, analyzing, and embellishing the data, such as adding mapping, and presenting of the information to the user. This model is used by some modern self-tracking devices. Many of the wearable tracking devices do not have full function information displays. Instead, they often just use a number of LEDs to indicate essential status information only. The key to unlock the usefulness of this type of system is the smartphone app, which processes and presents the data back to the user.

Note: A smartphone in this context could also be a desktop or laptop computer with Internet access.

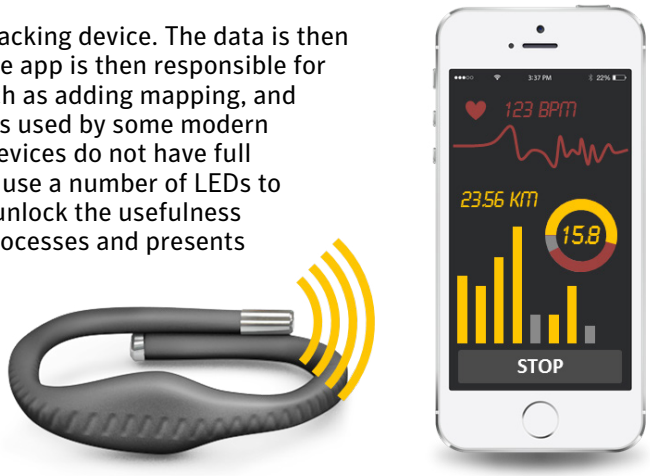


Figure 13. Example of a wearable device that transfers collected data to a smartphone app

Tracking device + cloud

In this model, the wearable tracking device collects data and then the data is transferred directly to a cloud service which is responsible for storing, processing, and presenting the data back to the user. In some instances, the device may also be able to perform limited processing and displaying of data to the user but the real value is gained when the user logs onto the cloud service to review the processed information.

Devices in this category can directly access the Internet to transfer data.

Note: A wearable device in this context could also be a stand-alone self-tracking device with direct Internet access.

Figure 14. Wi-Fi scales that can transmit data readings directly to the cloud

Smartphone app only

In this model, an app is installed on the smartphone and the app uses the various built-in sensors inside the smartphone to track and monitor the activities of the user. Today, it is common even for lower end phone models to have a range of sensors such as accelerometer and GPS built in.

This system model does not use online cloud storage of the data. Instead, all data is stored and processed locally. This is a relatively uncommon way of doing things as most service providers today are realizing the value of user data and are aiming to capitalize on the data that their users are generating.

Using a relatively advanced device such as a smartphone to collect, analyze, and display data is not a major disadvantage for self-tracking and has advantages for privacy. However, users may find it useful to view an analysis on a larger screen or have the data backed up to the cloud in case there is a need to upgrade to a new device or if the smartphone gets misplaced.

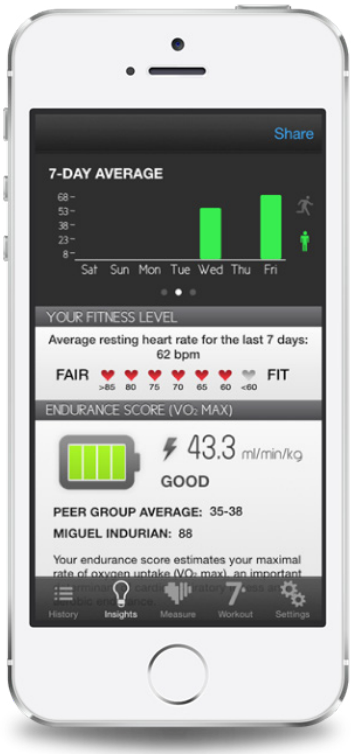


Figure 15. Cardiio is a typical smartphone only quantified self tracking app

Resources

Symantec Internet Security Threat Report 2014: Volume 19
http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

File Your Taxes Before the Fraudsters Do
http://krebsonsecurity.com/2014/02/file-your-taxes-before-the-fraudsters-do

Big Data Is My Copilot: Auto Insurers Push Devices That Track Driving Habits
http://business.time.com/2013/08/06/big-data-is-my-copilot-auto-insurers-push-devices-that-track-driving-habits/

Social Networking Increases Burglary Risk
http://www.telegraph.co.uk/travel/travelnews/10171799/Social-networking-increases-burglary-risk.html

Wearable Technology – Market Assessment - IHS.com
http://www.ihs.com/pdfs/Wearable-Technology-sep-2013.pdf

The Tangled Web of Password Reuse
http://www.jbonneau.com/doc/DBCBW14-NDSS-tangled_web.pdf

Why Your Web Site's Privacy Policy Matters More Than You Think
http://www.businessweek.com/smallbiz/running_small_business/archives/2009/08/why_web_site_pr.html

Anonymity, Privacy, and Security Online
http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf

Build Security In
https://buildsecurityin.us-cert.gov/

Common Weakness Enumeration
http://cwe.mitre.org/top25/

Handbook for Safeguarding Sensitive Personally Identifiable Information (DHS)
http://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf

Session Management Cheat Sheet
https://www.owasp.org/index.php/Session_Management_Cheat_Sheet

Here's Why You May Never be Truly Anonymous in a Big Data World
http://www.nextgov.com/big-data/2014/07/heres-why-you-may-never-be-truly-anonymous-big-data-world/88492/

Obligations of Data Controllers
http://ec.europa.eu/justice/data-protection/data-collection/obligations/index_en.htm

Bluetooth Company Identifiers
https://www.bluetooth.org/en-us/specification/assigned-numbers/company-identifiers

About Bluetooth Low Energy Technology
http://www.bluetooth.com/Pages/low-energy-tech-info.aspx

SIT Technical reports on The Security of cloud Storage Services
https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Cloud-Storage-Security_a4.pdf

Data Dealers. Collecting, Collating, and Selling Personal Data Background Information and Research
http://datadealer.com/datadealer_backgrounds_research.pdf

Data Protection Laws of the World Handbook: Third Edition
http://www.dlapiper.com/en/us/insights/publications/2014/01/data-protection-laws-of-the-world-handbook/

Enhancing Cloud Security Using Data Anonymization
http://www.intel.com/content/dam/www/public/us/en/documents/best-practices/enhancing-cloud-security-using-data-anonymization.pdf

Best Practices for Mobile Application Developers
http://www.futureofprivacy.org/best-practices-for-mobile-app-developers/

Authors

Mario Ballano Barcena,
Candid Wueest,
Hon Lau

About Symantec

Symantec Corporation is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings - anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenues of $6.7 billion.

To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com