TABLE OF CONTENTS

CLOUDY WITH A CHANCE OF STORAGE

Data is power

The many parties busily collecting data about us, are literally collecting power. A party that knows a lot about us can use that knowledge in ways that are not in our own best interest. Unfortunately, for many people the risks associated with 'Big Data' are still not clear.

Roughly speaking, the dangers lurk in two distinct areas. The first area is not so hard to recognise, certainly not once you've experienced it: it's the area of crime.

A well-known and probably the most shocking example of the dangerous power of data is offered by the Second World War. Before the war, every municipality kept a population register that also recorded to what faith a person belonged. Handy, perhaps, until it turned out to give the occupying forces direct information on who was a Jew[14]. This made the process of rounding up and deporting Jews a simple matter of 'running down the lists'. The crimes of the holocaust may be considered one of the most horrific cluster crimes ever committed.

Closer to home, in contemporary life we encounter all sorts of identity theft, fraud and blackmail. Lots of people were blackmailed after the membership list of dating website Ashley Madison, whose services help people cheat on their partners, was hacked and made public[15]. That a lively trade exists in stolen credit card data is no longer a surprise. These unwelcome consequences of the information age are easy to understand for most people, as they resemble things we were already familiar with.

EXAMPLE

Ashley Madison
In 2015, the membership list of the Ashley Madison dating website was hacked. The goal of this dating website is to link up people seeking to cheat on their partners. The site had some 30 million members[16]. The list was then made available to the public, with fairly drastic consequences. Innumerable relationships were wrecked, and at least two people committed suicide.

The second danger posed by "Big Data" is not of a criminal nature, but can have severely negative consequences for society. Technologies that enable the delivery of highly personalised services also enable new and subtle forms of discrimination[17]. For instance, the price people pay for insurance policies is increasingly determined by an algorithm that reaches certain decision based on pre-programmed generalisations. Thus, someone moving into a neighbourhood with a high percentage of residents

BIG DATA
IS
WATCHING
YOU

Think about how you want to deal with privacy and data during the very first stages of the project. Hopefully this sounds obvious, but in practice it's usually not how it goes. In many products, privacy features are only incorporated in a later stage, in the worst case following public protests. At that point it often poses a challenge, for instance because the software cannot be modified anymore, the hardware infrastructure is prohibitively expensive to adapt or replace, or because the chosen business model cannot allow it. At times the violation of privacy is deliberately built-in, for instance by using so-called 'dark patterns', to achieve that people give away more information that they realise and would want to. A lack of will, bureaucracy and a lack of knowledge make it difficult to adequately tackle these problems. By focusing on and examining the issue from the outset, these problems can hopefully be prevented or solved as effectively as possible.

→ Dark Patterns p.123

An interesting example is the FindFace app. If you use it to take a picture of a Russian, it will find that person's account on the Russian social media website VKontakte. This has led to the stalking of women whose nude pictures were posted online, and has led to vigilantism in a case where arsonists were found by the public when they fed the app security footage.

All this is possible because the VKontakte website makes it very easy to have access to the data of their members. While this helps programmers make apps on top of the social network, it also leads to often foreseeable excesses.

A poor design can even be life-threatening. In 2015 it emerged that it was possible to take control of a new model of Jeep cars via the internet, for example to apply the brakes or turn off the engine remotely[51]. The only way to update the software was to insert a USB stick with the update in the car dashboard. Chrysler, the parent company of Jeep, then decided to recall 1.4 million Jeeps. It is another example of the astounding lack of consideration for the privacy and safety issues that may occur during the full usage cycle of a product or service.

This particular type of problem didn't emerge just yesterday. According to a recent estimate by researchers of the French knowledge centre Eurecom and the German RuhrUniversität, around one quarter of all devices and appliances connected to the internet are very easy to take over remotely[52]. Part of the problem is that these devices can often be accessed using the well-known standard passwords.

Most problems will not be solved quickly Manufacturers are often slow to offer updates because it costs a lot of money. Android phones in particular are prone to this problem. In other cases a solution is available, but doesn't make it to the system. For instance, the solution for the Jeeps, as described above, required the manual insertion of a USB stick in the dashboard. In such cases, there will always be a proportion of devices that users fail to update[53]. In the worst case the product flops, reaches 'end of life', or the business goes bankrupt. But the owners will still continue to use the devices.

Even a fully up-to-date device can turn out to be unsafe tomorrow, if hackers discover a new leak. Building software is and remains a human effort, with all associated weaknesses.

So lots of things can happen during the lifecycle of a 'smart' product. It is important that a manufacturer and its design team can anticipate potential problems and respond quickly if the problem becomes real. This can be achieved by designing manuals and processes that allow the customer to act when required, for instance in the case of a hack. Manufacturing processes should deliberately

EXAMPLE

The National Birthday Calendar
In 2016 the Dutch media lab SETUP wondered how difficult it would be to follow in the NSA's footsteps and create a database of all Dutch citizens, simply by gathering public data online? Would it be possible to use that data to develop a service that helps everyone remember birthdays, and even offer intimate gift suggestions based on their interests? With the help of 30 data professionals they spent six Saturdays making this data-puzzle based on old social network data, the phonebook, the local version of classmates.com, websites of professional associations and sports clubs, and so on. This not only proved possible, but even surprisingly easy: none of the websites resisted the large scale copying of their data.

Other forms of crime are more targeted. The American family Straters was terrorised for years on end by a cybercriminal named Kivimaki[63]. He had pizzas and other delivery services come to their door (for which they would have to pay), had their electricity cut off remotely, and made false phone calls to trick the police into paying them heavily armed visits. The resulting stress for the family was so great that it ultimately resulted in the parents' divorce.

Most people will immediately associate 'hacker' with 'criminal', but experts distinguish two types of hackers: white-hat and black-hat, or "ethical" and criminal hackers. In every large city you will find "Hackerspaces": club homes where ethical hackers convene. They are often available to help you with all your technological questions.

Hackers nowadays play an important role in the design of digital systems. They are happy to point out all the flaws and leak holes. Many hackers are driven by social concerns: aside from the practical dangers of identity theft and other criminal misuse, they also remind us of the larger social issues. Ethical hackers form an important part of digital society's conscience, and often act in the awareness that this society might well become a whole lot less 'sociable'.

If you prefer to meet the institutionalised hackers' world, then search for 'ICT security audit' companies.

Think like a hacker! Let's conduct an experiment and make a list of the types of data that are frequently collected, and then examine all the possible ways in which this data could be misused.

at the front door before he even rings the bell[68].

This is a violation of the pizza deliverer's privacy. He/she can no longer choose to vary the route without running the risk of having to explain this to the boss, while there are various legitimate reasons why one might want to do so: for instance for religious reasons, in order to collect medicine from a pharmacy, or for social reasons. If your response now is to think, 'but then you can just say so', then you're missing the point: without anthropological research, chances are that certain culturally sensitive, practical or unforeseen situations arise that you cannot foresee with your limited knowledge.

We can devise solutions that work for everyone and that store less data. The customer doesn't care about the mileage involved in delivering his pizza, but the number of minutes. With modern navigation algorithms, calculating approximately how long it will take the pizza to arrive is no effort. By indicating only the amount of time it will take for delivery, both the customer and the boss have less privacy-sensitive information in their systems.

There are many more situations in which a bit more thought, and a bit more of a critical attitude, can result in a solution that serves both the privacy interests and the design, and the operational processes.

PRINCIPLE 4

PROTECT YOUR DATA

You will want to collect information on how whatever you create is used in practice. Saving that information in ‘the cloud’ can be tempting or even become unavoidable. But it should never become a matter of course.

‘The cloud’ is in fact a pretty name for ‘someone else’s computer’. Terming it this way helps bring out the tensions involved: who does the computer belong to? In what country is the computer kept? Many critics have pointed out that terms like ‘cloud’ and ‘cyberspace’ are misleading, as they make us think that the internet is a place that transcends borders and politics. But someone else’s computer is always in a particular country, and subject to that country’s particular laws on privacy and data property.

Some countries pursue an active policy in this respect. For example, Iceland promotes itself as a country where journalistic freedom also extends to the internet. Ireland is another popular country for the storage of a large quantities of data, thanks to its flexible local regulations.

The first question every designer should ask is: is it essential to store these data in the cloud (on someone else’s computer)? For example, take fitness trackers. These have access to highly personal information, and in many cases this information is automatically sent to ‘someone else’s computer’, for instance to facilitate sharing that information online. In theory, however, there’s no need to upload the data to the internet. Fitness trackers could also save the data locally on a smartphone, from where it can optionally be compared or enriched with other data obtained from the internet. It would also still be possible to share the information on social networks.

If the data is stored online, the question is in what country it is stored. In theory, the European Union offers the end user better privacy protection than the United States[69].

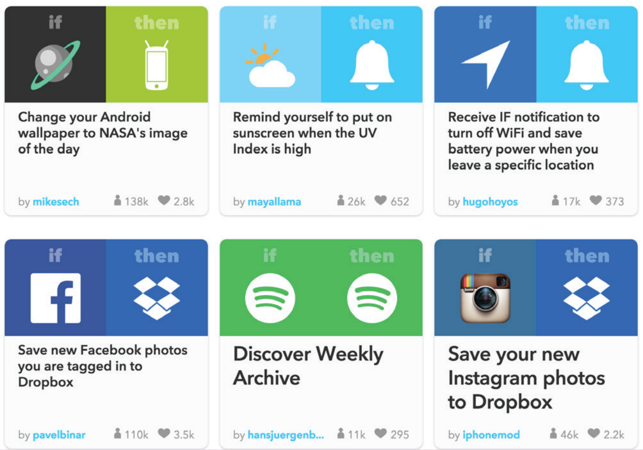
EXAMPLE

The Citizen Ex project by James Bridle
The Citizen Ex project displays the physical location of the websites you use. The art project generates a new flag, in which the flags of the countries where your data is kept are merged together. It won’t surprise you to know that many of the popular services are run on servers based in the United States.

Finally, it should be a matter of course to store data in encrypted form. Lots of books have been written about data encryption, as hiding data has evolved into a true mathematical art. There are numerous ways to do it, with solid encryption standards now available for the most common scenarios. Use them, and distrust anyone who proposes to develop a new standard[70]. These standards

If smart products and services are easy to adjust, then end users can take care of this last bit of ‘customising’ themselves.

All sorts of promising new interfaces are emerging that play with this principle. One good example is If This Then That: a website where people can link up services in a way that resembles a strongly simplified form of programming[83]. In a world where almost everything in our environment has a technological component, it’s not a bad idea to teach everyone a little bit about programming, so that everyone can understand something of how all these devices work.



Change your Android wallpaper to NASA's image of the day
by mikesech 138k 2.8k

Remind yourself to put on sunscreen when the UV Index is high
by mayallama 26k 652

Receive IF notification to turn off WiFi and save battery power when you leave a specific location
by hugohoyos 17k 373

Save new Facebook photos you are tagged in to Dropbox
by pavelbinar 110k 3.5k

Discover Weekly Archive
by hansjuergenb... 11k 295

Save your new Instagram photos to Dropbox
by iphonemod 46k 2.2k

Examples of recepies on iffttt.com

In a world immersed in network technology, designers are challenged to embrace this educational role. Instead of producing finished products that simply work automatically, we should develop Lego-type interfaces[84]. That would give the user some control over the behaviour that our creations can display, in a user-friendly fashion.

Especially the complex behaviour that can arise from the interaction between systems is otherwise difficult to understand and control.

In the ideal scenario, a society will emerge in which people view technology much like they now view cooking. The fascination we all have for cooking is actually quite strange, as we might consider cooking a ‘problem solved’. After all, since the microwave and ready-to-eat meals were invented no one needs to cook anymore, and you can simply rely on the cooks of those meals and on the market producing the microwaves and meals. But the real world is a very different place, in which people prefer to prepare their own meals and look down on microwave food. We love to cook, as a fun and rewarding activity. We concoct our own recipes and adapt dishes to suit our own taste. People with a knack for ‘programming’ food (= cooking) are even considered sexy.

Just like you would want to adapt a traditional interface to suit the user’s culture (larger buttons for elderly people, for example), you would want to adapt the behaviour of the smart environment to the local situation. To do so requires the help of the user, however. But then the user must have the courage and knowledge to do so. Ease of use and simplicity are commendable, but we should always challenge users to continue to learn and discover more about what’s possible, and so to turn him or her into a co-designer of his or her own smart environment. This is an immense and almost educational challenge for which new forms of design must be developed. If we neglect to do so, then dependency will increase, and the digital divide will deepen[85]. → Affordance, p.120

Privacy product analysis

Privacylabel

GOOD DESIGN

DUBIOUS DESIGN

BAD DESIGN

Product Xiaomi Mi wrist band

PRINCIPLE 1 It is difficult to determine to what extent Xiaomi considered privacy issues beforehand. It has a questionable reputation in this regard[93]. The following points also suggest that privacy and safety were not treated with the care and attention they deserve.

PRINCIPLE 2 The risk of creative misuse doesn't seem to have been a worry, given its poor protection. We should realise here, however, that European and Chinese standards and values diverge significantly. What we might see as unwelcome surveillance, they may consider proper control.

PRINCIPLE 3 The wrist band continually collects data, as required by the promised functionality. So that's clear. It also measures just one thing, namely motion, so that's fairly simple. However, Xiaomi appears to transmit all the data to its servers, and not just a summary, which should be more than enough, theoretically[94].

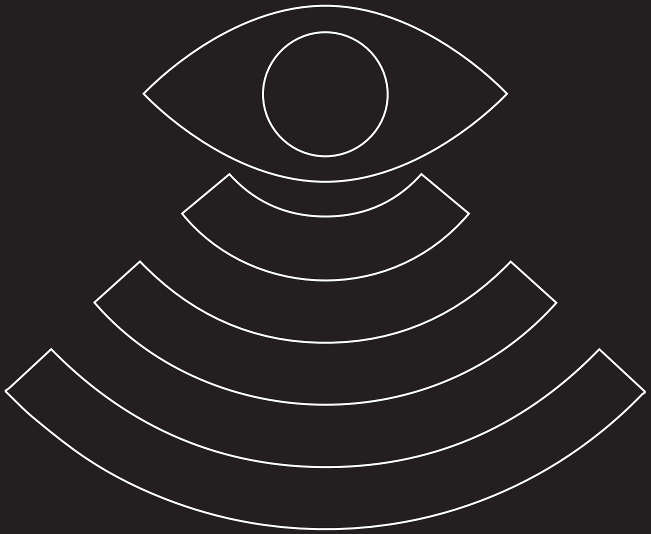
PRINCIPLE 4 The data is not stored on the app or smartphone in encrypted form[95]. Hobbyists have developed bits of software that enables the retrieval of data from the telephone. Hopefully the data is stored in encrypted form on the server, but even that would only discourage data theft. The Chinese government arranges the access to the data. This is possible because Xiaomi possesses the encryption key and will share it with the government. So the government can find out what your daily life rhythm is like. One positive note: the connection with the server is secured.

PRINCIPLE 5 The app forces the user to create an online account, but there is no need to use your real name[96]. But why the need to create an identity and to communicate with a server at all? If used anonymously, the wrist band would still generate the same insights.

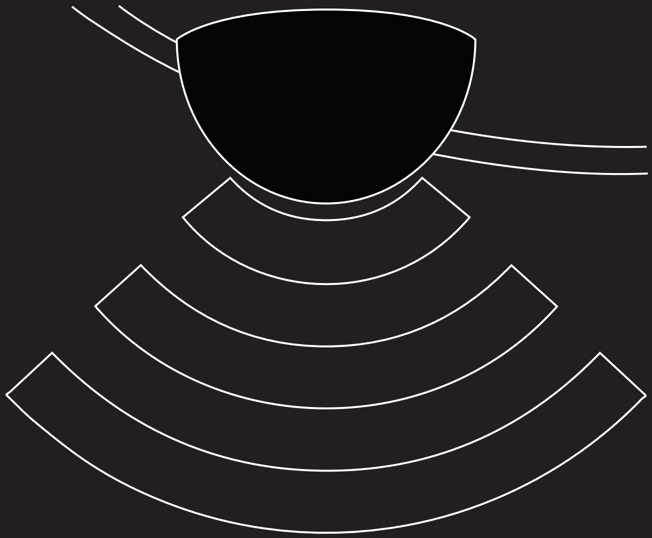
PRINCIPLE 6 It isn't clear exactly how the algorithms do what they do[97]. How does Xiaomi define 'deep sleep'? Why not explain the operation of the algorithm in the user's manual? How can you communicate the concealed preferences of an algorithm to the user? These are design questions that are left unanswered.

PRINCIPLE 7 Your data is sent to Xiaomi's webservers. You have no choice in the matter.

PRINCIPLE 8 The prescriptive abilities of the Mi-Band seem limited, because the device cannot be linked easily to other services. It is unclear how the algorithms differentiate deep sleep from light sleep. The device does not take one's overall health condition into account.



WATCH
OUT
FOR



NOT
BEING
WATCHED