D/SRUPTION

HOTWIRE
THE GLOBAL COMMUNICATIONS AGENCY

Foreword

"Fortunately, as consumers we are rapidly coming round to the idea that it would be a good thing if we had more control over our data"

Do we ever really know what we're giving up when we sign away on those online T&C's? Personally I feel pretty smug when I work out if the "can we sell your data" checkbox should be ticked or left depending on their sneaky wording of the question. I am naively safe in the knowledge that my email address (and maybe more) is nice and safe in a datacentre somewhere, protected by 17 levels of firewall and encryption.

I considered myself to be pretty savvy having worked in tech for 20 years, but it wasn't until I heard Nicholas Oliver at People.io talk on the topic of privacy that the real deal became obvious: your email address is rapidly becoming the least interesting bit of data you hand over. When you ticked "accept" in those T&C's, you opened up an unbalanced value exchange so big that it will blow your mind.

Fortunately, as consumers we are rapidly coming round to the idea that it would be a good thing if we had more control over our data and this is beginning to have a profound effect on how online and offline services are shaped. Those brands with a strong story to tell its customers around increased autonomy and privacy will get the jump in this new data-aware world and in turn this will fuel a huge increase in demand for the underlying technology which powers these controls for service providers. So whether you're a tech vendor or a brand looking to build sustained loyalty, getting your story straight on privacy has never been more important to your future success.

/ Matt Cross
Managing Director Hotwire

How much privacy do you really have? ...You probably don't know.

Across society, privacy is considered a basic right. But digital disruption has brought with it a new concept – data as commodity. As profit expands from 'product only' to 'product and data', information is where true value lies. As a result, the meaning of privacy has changed.

What is privacy?

Privacy is the right of an individual or group to keep information about themselves from another party. At one point in time, this meant locking your front door or deleting your internet history. Now, things are not so simple.

Due to the accessibility of vast amounts of data, privacy can no longer be taken for granted. In fact, it is fair to assume that any information about you that has ever entered digital form could be accessed by somebody at some point in time. This has led increasingly to the idea that consumers should have digital sovereignty – in other words, digital data and presence should be entirely under consumer control.

Why is privacy important?

"But with every move we make in the digital sphere, we leave a trail of personal information."

Privacy is a cornerstone of legal and social protocol worldwide. But with every move we make in the digital sphere, we leave a trail of personal information. These breadcrumbs are collected by the platforms and organisations that we interact with, and for the most part it is difficult to know exactly what they are used for. Case in point: Uber.

Through location services, Uber is able to track your journeys. The company knows, for example, that you use the app every Wednesday at 7pm. Divulging your personal routine to a corporation is problematic enough, but at one point Uber also knew where its users were even when they weren't using the app. While data use should be outlined clearly in the terms and conditions of any technology, that information is still hard for users to fully understand the implications in some instances. Furthermore, many people still consider this a gross violation of their right to privacy… even though they will have agreed to it on sign up.

Privacy is especially important today because the information we put out into the world shapes our experiences and our opportunities. On an individual level, it can dictate the content that we see online, creating tunnel vision.

Now as we are inviting technology into our lives with connected devices like Google Home and Amazon Echo. The platforms listen to users, and respond to them, while collecting accurate data on how we live our lives. Through wearable devices, we can track our physical health and wellbeing. If this information was accessed by an insurance company, or by an employer, the consequences could be vast. Before mass data and digitalisation, privacy was a given. Today, it is a luxury.

People and privacy

"The problem with privacy is that the boundaries are decidedly unclear. At what point does your data become someone else's data?"

In order to receive products and services from most corporations, consumers are required to part with privacy. In many respects, exchanging privacy for quality can be advantageous to all. We know that data powers the products and services that we use, and we know that if we hand over a proportion of our personal data those products and services will work better for us.

Unfortunately, this has led to an apathy regarding data ownership that has, in part, allowed organisations to take advantage of consumers. This can be partly attributed to the fact that many people don't realise the potential implications of what their data trails could mean for them further down the line.

The problem with privacy is that the boundaries are decidedly unclear. At what point does your data become someone else's data? What can they use that data for without your permission, and who can see your private information? What are corporations doing with your data, and how does it affect your life?

The answers to these difficult questions all begin with an awareness of what data you put into the world as an individual. Familiarising yourself with the data policies of the corporations you regularly use is a good place to start.

The threat from cyber criminals

"2018 showed increased collaboration between cybercriminals in underground alliances, and this trend is predicted to continue."

When consumers interact with an organisation, their data is scooped up and stored in a variety of locations. One of the main issues with data privacy is how that data is used by the organisations that collect it... But what if that data is stolen by an external, malicious influence? As sophisticated cyber criminals refine their techniques, losing customer data as a result of cyber crime has developed into a very real threat.

According to the McAfee Labs 2019 Threats Predictions Report, cybercrime will become more innovative and agile over the coming year. 2018 showed increased collaboration between cybercriminals in underground alliances, and this trend is predicted to continue. As a result, major companies are expected to experience a rise in attacks.

Not only does this threaten the privacy of the company, but the privacy of its customers too. Without an appropriate response system in place to deal with cybersecurity breaches, organisations are at risk of losing consumer data. Losing people's data means losing their trust, ultimately damaging brand image. This is a challenge that question-and-answer website Quora now faces after hackers stole data from an estimated 100 million users. This included their email addresses, encrypted passwords, user account settings and IP addresses.

It's not just big businesses that have a responsibility to address the threat from cyber crime. Smaller organisations are as much at risk of data breaches – partly because they are less likely to put the necessary protocols in place to detect and deter hackers. Regardless of size or industry, companies need to accept that cyber attacks are becoming a harsh reality. This is also something that individuals should be more attuned to. The moment data is shared, it becomes a valuable asset that, just like any other asset, can be stolen.

Can privacy exist in a data driven world?

Following a string of corporate blunders and the prevalence of cyber attacks, data privacy has become a pressing public concern. Fortunately, there is now more demand for organisations to be transparent about their data collection and use.

In May 2018, the EU's General Data Protection Regulations forced all companies to reevaluate their data strategies. While GDPR can be viewed as a necessary and positive development, it has been criticised as stifling innovation. On the one hand, consumers have more say over their data, but on the other, companies have lost out on potential insights that could improve their operations. There is a difficult balance to be struck.

In light of so many uncertainties, is privacy possible? Yes, through education, discussion, understanding the value of data, and what can be done to protect it. There is a responsibility for regulators to force organisations to face up to the data debate, and prove that they can be trusted to use information benevolently. At the same time, it is also up to individuals to move from apathy to awareness. If you are sacrificing privacy, it has to be worth it.

5 Key Considerations

Understanding privacy in data driven markets is a legal, economic and social dilemma. Conversations surrounding privacy are still largely in their infancy, especially from a consumer perspective. However, the wheels are in motion towards showing people what their data can do for them – without compromising information that they want to keep to themselves.

Develop awareness

Navigating the complicated world of digital information begins with a baseline awareness of what data is available, and what that data is being used for.

Accept responsibility

Business have a responsibility to protect the data they collect, but it is also up to individuals to consider the potential implications of their personal information.

Data as permanent

Intelligent software platforms are trained on data that, even if deleted, will retain a presence. Viewing data as a permanent record could help to combat data complacency.

Change the language

As long as corporations set the boundaries of data collection, use, and protection, they will remain in control.

Expect regulation

GDPR represented an important initial step towards data transparency, but organisations should be ready to face more legislation.