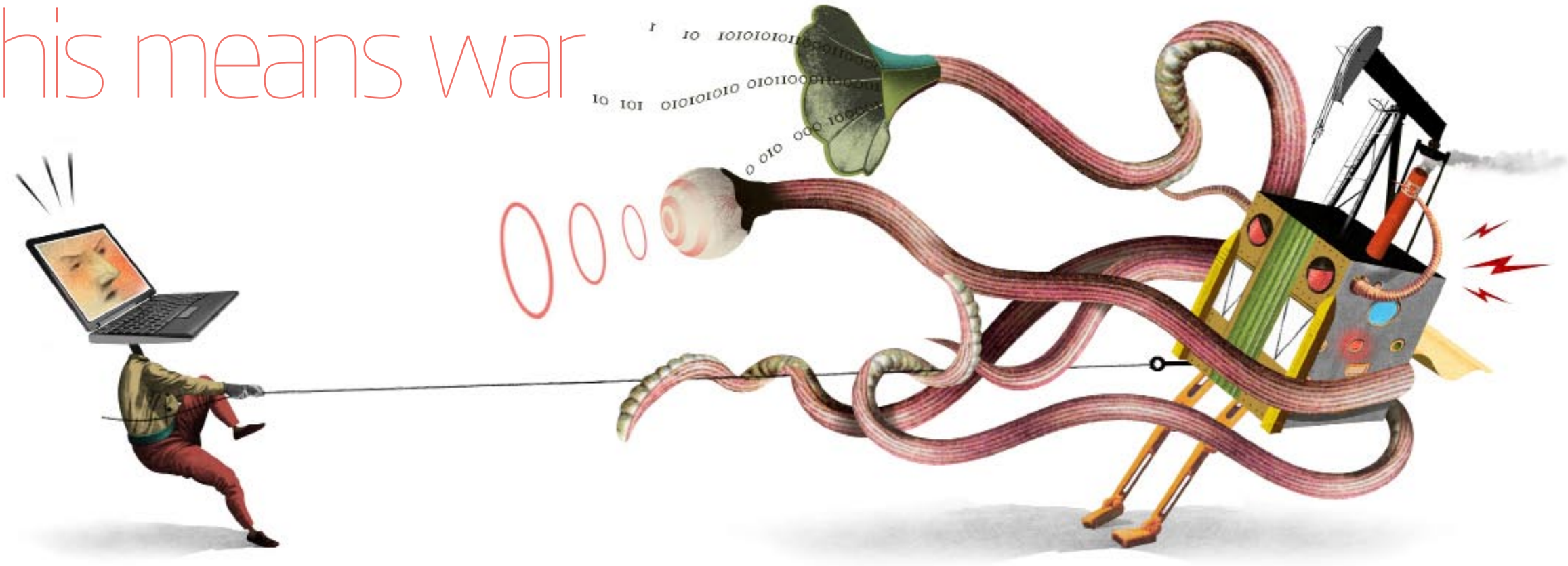
This means war



We have no control over the pieces of ourselves we give away daily and freely in exchange for a superconnected world, says MacGregor Campell. Time to claw it back

MY new loyalty card looks just like any other store reward card. With a quick swipe whenever I buy groceries, I give the supermarket permission to track my buying habits in exchange for those nice lower prices posted throughout the store.

It seems like a good deal – hey, I got free eggs just for signing up – but will I come to regret my decision?

When I signed up for the card, I ticked a box that allows the store to use my data in accordance with their privacy policy. I did the same thing many dozens of times last year, every time I signed a website privacy policy, warranty card, or credit card application, none of which I took the time to read. Once set loose into the world, the data I gave them permission to use joined the slipstream of information about me emerging from a host of other sources – including social networks and even local governments – all of which allows "me" to be sold at a nice profit.

At first you may not see how any of these data points can have any value. But collated, packaged, and sold to the highest bidder, "you" and "me" seem to be making a lot of people rich. Everyone, that is, except you and me. In fact, we have essentially no control over that data: who uses it, how they use it, and what they do with it.

That's largely due to the fact that most of us wouldn't know where to start keeping track of all our information. But our lack of control is starting to have unpredictable and sometimes unpleasant consequences. A new group of companies is on the rise that promise to help us wrest back control over a resource that was arguably always ours to begin with. We might even be able to profit from selling ourselves.

Just by being alive in a hyper-connected world, each of us is a wellspring of increasingly intimate details. In the bricks-and-mortar world, there is voter registration information, property records, credit scores and transaction histories. Then there are the "cookies", software that collects the breadcrumb trail of our web browsing, usually without our knowledge. Your mobile provider keeps track of your locations, calls and text messages. And of course the Tweets, likes, and profile interests we offer up.

This welter of information is the lifeblood of an ecosystem that comprises hundreds of companies large and small, all of which make a living compiling this information into a dossier on each of us. Some of these, such as Acxiom, which is based in in Little Rock, Arkansas, and Dunnhumby, are international conglomerates that aggregate global data. Others, such as San Francisco-based RapLeaf, focus on their own countries. All of these so called data aggregators vaccuum up the world's discrete pieces of information about you, place them into their giant databases and and sort you into a behavioural category, wrapped up neatly and labelled with your email address.

You might recognise yourself in Axciom's classification system, say, as a Married Sophisticate – a recently married early 30-something who owns her home, watches Mythbusters, and is still paying off college debt. Or perhaps you are a Midtown Minivanner – a working parent in your early 50s who enjoys courtroom reality shows and avoids online banking. Can't find yourself? Try any of the other 70 Acxiom categories. Rapleaf cuts a picture of you from about 400 variables.

Who is interested in these profiles? The biggest data aggregators make their money by selling profiles, for a hefty profit, to the likes of Federal Express, HSBC and department stores that want to know exactly how much the people in your category are willing to pay for those trainers. This is the fuel of the internet economy, and it is why search, social networking and many apps are free.

Data mine

There have always been people who cried foul. "What we see is this commercial surveillance industry that has sprung up in the last decade and a half," says Peter Eckersley, a director at the Electronic Frontier Foundation, a digital rights advocacy group in San Francisco. However, many of us seem untroubled by the intrusion. In 2009Aleecia McDonald at Harvard and Lorrie Cranor at Carnegie Mellon University in Pittsburgh, Pennsylvania, asked participants whether they would be willing to pay $1 to keep their favourite new site from collecting data about them. Only 11 per cent accepted the deal.

And why should they? After all, the browsing data these companies collect isn't exactly incriminating. We only care about revealing private details when it has undesirable consequences, says Bernardo Huberman, a researcher with Hewlett-Packard in Palo Alto, California. In 2005, he found that, for example, heavier people want more money to reveal their weight if the audience will be a group of skinny people as opposed ›

PIC CREDIT HERE

to a group of people who are overweight.

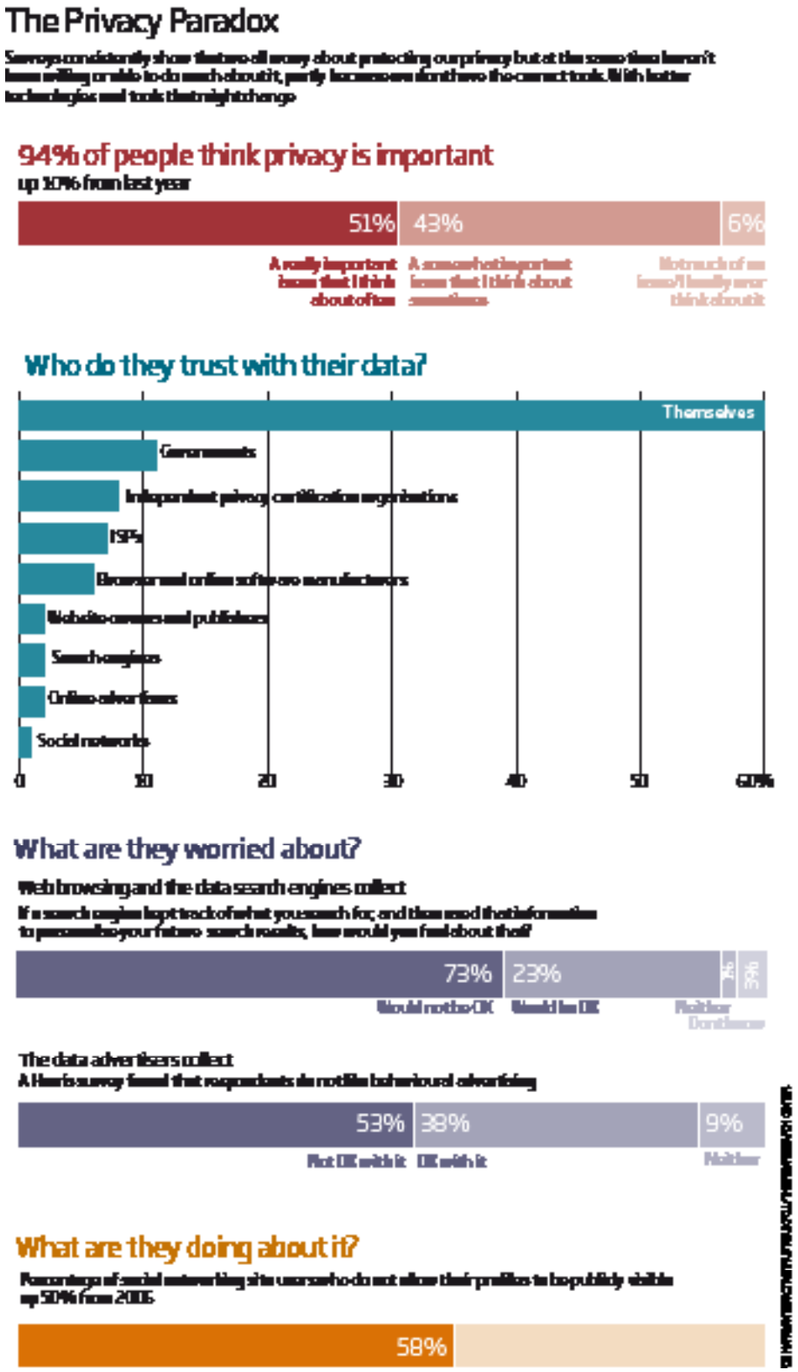
But over the last couple of years it has become clear that even innocuous data can incriminate. Companies can now avail themselves of your data to make judgments about, for example, your creditworthiness or insurance rates. In the US, reports have proliferated that insurance companies are using it to analyse who they should cover. Similarly, credit card companies were recently found to trawl data about where you shop to establish whether you are a credit risk. Scouring Facebook data led a US insurance company to deny mental health coverage to a woman whose status updates, executives said, belied her claim of depression.

Losing control

That's not all. Granular knowledge can lead to "behavioural pricing", a consequence experts began to worry about earlier this year. Your "personalised prices" would be a reflection of the frequency of your purchases. David Soberman, an economist at the University of Toronto, Canada, says while for now it's always in the form of discounts and special offers to seduce people away from competing stores, companies may eventually tap into such profiles to figure out exactly how much I'm willing to pay for those eggs. "You don't have to offer that attractive introductory price on something that people have already demonstrated that they really like," Soberman says. What is to stop them from using those proclivities to raise prices even more?

Public opinion has begun to shift. Earlier this year, a study conducted by Nicola Jentzsch of the German Institute of Research in Berlin asked students to purchase movie tickets – 83 per cent opted to buy from a vendor who didn't require their phone number. Jentzsch's findings are in line with a number of surveys published this year by Harris Interactive and Pew Research Centre: in a poll of 1000 UK adults, Harris found that 55 per cent are more inclined to do business with publishers and advertisers that give them the option to opt-out of sharing personal information.

Being aware of the problem, however, doesn't necessarily translate into doing anything about it, says Mary Madden at Pew Research. Survey respondents, she says, consistently cite concerns about their private data, but this attitude is not always reflected in their actions, such as setting social networking profiles to private, or using software that stops cookies. Then again, users may be chasing after moving targets: "The terms of



engagement with search engines, social media sites and other web sites are constantly changing, so the average user has a lot to keep up with," she says.

As McDonald and Cranor have found, it would take the average person almost 250 hours per year to read the privacy policies of the websites they visit in that time.

But the only way to keep information perfectly private is to stop generating it, which is next to impossible. Eckersley says you would essentially have to live like a criminal. Online, this would mean using ad-blocking programs, routing your internet traffic through proxies or anonymisation software and using pseudonyms whenever you sign up for a new online service. Offline, you would pay cash or use prepaid credit cards and prepaid cellphones – the untraceable "burners" most often associated with drug dealers who throw them away after the minutes are up. "Basically the industry has refused to provide a way for people to opt-out of being tracked in any sensible way," he says.

Governments are attempting to protect consumer rights online. Earlier this year the Obama administration unveiled a privacy rights bill. The European Union recently began to enforce a ban on cookies, and Google has promised to put a Do Not Track option into its Chrome browser. However, Eckersley says many of these measures are toothless.

Battle royale

In response, new companies have sprung up tools to take control of your data. The easiest way to do it is to sow confusion about its accuracy. Breadcrumbs, an online service registered in Israel, helps you throw the data hounds off your trail with a feature called "Bogus Identity" which dilutes your valuable data with large volumes of false information. The tactic is known as "data pollution".

If digital smokescreens aren't your cup of tea, there are other options. As the Pew poll revealed, most internet users say they do not know how to limit the information that is collected about them by a website. Palo-Alto-based Privowny has a solution for in the form of a browser plug-in that keeps track of the data you provide online, letting you update or delete information across multiple sites.

For now, this will only work for data you enter after the software is installed, but the company says it is working on a way to gather all your information across the internet – from Facebook, LinkedIn, and others – to give you access to your full internet dossier, something

> "It would take almost 250 hours per year to read the privacy policies you sign each year"

that for most people is now impossible. While current laws allow people to review and challenge errors in their credit histories, there now exists no way to fact-check your data file.

Another class of privacy protectors is emerging that may shake up the market. A spate of startups with names like Personal, Singly, MyDex, and Azigo provide "data locker" services that allow users to enter their information explicitly and then control who can access it. They are circling around a new paradigm: an economy based on letting you benefit from your own data.

We are, after all, sitting on something valuable. "Right now, everybody's monetising your data except for you," says Josh Galper of Washington DC-based Personal. But people are becoming aware that their data is actually worth something.

In research to be published, Sarah Spiekermann, at Vienna University of Economics and Business, Austria, asked 1000 online participants what they would do if their Facebook profile were to be deleted unless they paid to keep it or allowed it to be resold to a third party (*Thirty Third International Conference on Information Systems,* Orlando 2012). It turned out that people would rather delete their entire Facebook profile, with all its contacts, photos and history, than make it available to third party marketers.

However, Spiekermann says attitudes changed when money was offered: "As soon as people learn that there is a market out there for their personal data, they want to be paid".

Personal and Privowny have plans to work with partners who will do just that, most likely in the form of discounts at first. It might be a shopper loyalty card that works for whatever stores you like, where you get to decide the terms of service – or even get royalties. Each time someone used your information, for example, you might receive a micropayment.

You might think the biggest hurdle would be getting data aggregators to pay us instead of each other. But personal data services would benefit both us and businesses, says Doc Searls of Harvard's Berkman Center. The companies need clean, accurate data. Information gathered about us without our knowledge can be misleading because it lacks context. Store loyalty cards, for instance "can't tell that a vegetarian only bought hot dogs for a school picnic," he says.

Searls thinks we may be able to turn the current system in which companies compete for our attention by using flawed data to guess at what we might want into an economy where we get to decide exactly what we want to reveal and to whom.

Not everyone agrees that these companies will thrive. Princeton computer scientist Arvind Narayanan recently questioned whether shifting control from centralised businesses to individuals was feasible or desirable. He pointed out that many of the valuable services that credit card companies, for example, now perform using personal data – most notably fraud detection – don't work as well on decentralised data sets.

There are other challenges. Avi Goldfarb of the University of Toronto, Canada, cautions that some technical problems remain before we can all sell our own data. "When you give data to someone, you don't have to give it up," he explains. "This makes it difficult to enforce ownership rights."In other words, Personal can instruct a third party that your data is only good for one transaction, but the third party doesn't have to listen.

But even if the future does not lie with the specific companies now hawking their wares, Bernardo Huberman thinks change is afoot. He envisions a different future of data trading, an open market similar to eBay where we offer our information at different prices based on our attitude to privacy. In May, Huberman published a study describing how to price data in this theoretical marketplace and says that several EU companies have approached his lab to find out if such a marketplace is feasible.

However it happens, the era of the uncontrollable data-gusher looks as if it is coming to a close. Within a few years, my supermarket might need to prove its loyalty to me. n