theguardian

Five strategies for reclaiming our personal privacy online

Emily Taylor

Our privacy is being exploited commercially by the oligopoly of Silicon Valley, and in the name of national security by our governments. With so little control over our online lives, how can we reclaim the balance?

Thursday 26 November 2015 14.34 GMT

When Tim Wu published his influential book Master Switch in 2010, he powerfully argued that all communications markets began with a period of creative openness and experimentation, yet within 20 years settled into some sort of state-regulated oligopoly. The internet, Wu proclaimed hopefully, could be different because most internet giants “profess an awareness of their awesome powers and some sense of attendant duty to the public”.

Five years on, and it is becoming increasingly obvious that the web *is* now ruled by oligopolies, and that attempted state intervention is heavier than ever.

In technology markets it’s not so much a case of first mover advantage, but “winner takes it all”. Whether you’re in Austria or Yemen, Mexico or New Zealand, much of your online life is spent on three websites: Google, Facebook and YouTube. When Google had a one-minute outage in August 2013, global web traffic immediately dropped by 40%, according to web analytics company GoSquared.

Yes, the market is open in the sense that anyone can participate, but if you hit the rich seam and people like what you do, world domination seems to be the next step. The corollary is that the dominance is usually short-lived, overtaken by the next format or trend.

Terrorism too, usually motivates greater state control. Even in our outrage at recent terror attacks, we need to keep a cool head before enmeshing Big Tech even deeper into our surveillance machinery. As Paul Bernal warned recently, increased powers of surveillance and security should not be rushed through on a wave of emotion without proper scrutiny and consideration of farreaching consequences.

Both commercially and politically, these systems are challenging the rights of individual citizens by commercialising our online lives, and building a system that begs to be surveilled.

The legal fiction is that we consumers have agreed to this intrusion. But, as Al Gore observed, “every time we - collectively - have had a choice between convenience and privacy/security, we’ve chosen convenience.”

Why care? When companies share our data with governments in “cosy, voluntary relationships”, our civil liberties get nibbled away. With such powerful interests aligned, who’s looking out for the citizen? And what can be done?

1 Use of data needs to comply with human rights

First, governments need to ensure that Big Tech’s handling of our private data complies with international human rights standards - limiting intrusions to what is necessary and proportionate.

Human rights are the preserve of nation states. They stem from international conventions, which flow down into national laws and constitutions. Individual countries have obligations to protect, respect and fulfil human rights (the right to privacy, the right to free expression). Corporations can have a direct impact on human rights (think Shell in Ogoniland), but the usual legal frame is that countries are held accountable indirectly for the actions of corporations.

This seems to be lost in the online world. Though countries have the legal obligation to ensure freedom of expression, the internet is inherently international, so whose law applies? Private companies have filled that vacuum, evolving complex and secretive ways of moderating online content, including Google’s weird and opaque right to be forgotten process, and big tech’s content moderation operation, which is thought to involve as many as 100,000 humans looking at beheadings, porn and child abuse day in, day out.

Offline, nation states wouldn’t be comfortable with private companies determining standards of free expression and exercising censorship, with so little transparency. Yet online, they seem relieved that private companies are shouldering the burden of mediating the complex social, political and cultural challenges of global communications tools.

2 Different hierarchies of data

Al Gore, original champion of the commercial internet, now sees its darker side, calling it a “stalker economy”, where “customers become products, and business is collecting way more information than it should”. As the German paper Handelsblatt said, back in 2010, of one of the major internet players: “Google knows more about you and me than the KGB, Stasi or Gestapo ever dreamed of."

Different types of data need to be treated differently. Some things are inherently public and long-lasting - news articles, blogs and public records. We don't expect them to be private, and we expect them to last. Others are inherently private, such as email, because we wouldn't want strangers reading our letters. Big Tech is capable of fine-grained differentiation between different types of data when they want to remove posts that breach their community standards, because such gradation is essential to trust.

3 Data that naturally expires

We need aggressive deletion policies for stuff that, in the offline world, would just vanish into the air, like chat, or location data.

Once upon a time, web businesses struggled to convert web traffic into dollars. Then they struck gold: "free" services based on targeted advertising. The power of big data is awesome - and creepy. Automated analysis just of Facebook "likes" can accurately predict sexual orientation, gender, race, religious and political views, and use of addictive substances.

If you ever download your data from Facebook, you will find every wall update, photo and comment you've ever posted, and - creepiest of all - the text and time-stamp of every private message, every like, every share, ever. Things you'd forgotten, but Facebook remembers and exploits.

And while we have the illusion of control, because we can fiddle with our privacy settings, for the most part we can't opt out unless we stop using the service.

4 A paid option for the privacy-conscious

Fourth, many users don't care about what happens to their data, but for those who do, why not implement affordable paid options, with better privacy? The handful of popular services are now so ingrained in our daily lives that we need a more effective choice than total intrusion or total exclusion.

With userbases comparable to the populations of China or India, the providers' terms (the stuff we all click "I agree" to without reading) are effectively the law in Facebookistan and Googliana.

The terms nearly always give the provider unfettered access to our user data, including private chat, emails and location data; the right to delete or modify our data, including content, without notice; and the right to share it with law enforcement and advertisers.

5 Big tech needs more open discussions about ethics

As former GCHQ head, David Omand, said “Not everything that can be done, should be done”. We need a parallel track of ethics for the large internet platforms, an ethics body that could give guidance on deletion policies, content moderation and better consumer control over what is shared and with whom.

We keep pleading that the internet is different. Yes, the scale is vast. Yes, it’s international in nature. But if the outcome of these differences is that we trade our human rights for an ad-economy, then we as a society are paying too high a price for our free services.

- *Emily Taylor’s paper,* ***The Privatisation of Human Rights: illusions of consent, automation and neutrality*** *will be published by the Global Commission on Internet Governance in December 2015*

More comment

Topics

Internet

Privacy

Surveillance

Silicon Valley

Data protection

Save for later Article saved

Reuse this content