Cooperation between the communications industry and governments creates unprecedented opportunities for surveillance. Let's not repeat the mistakes of the past and allow companies to assume that users are uninterested in what happens to their data, urge Gus Hosein and Eric King of Privacy International.

Privacy advocates are often labelled luddites. Don't like a new service created by the coolest and latest billionaire geek-genius-led company? It's because you are a luddite. Don't like the government's latest technology for a new infrastructure of surveillance? Luddite. It's as though we are afraid of technology. It's because we understand these technologies better than most, that many of us became advocates in the first place. We need to know more about technology than the techno-fans. We need to know more than ministers promoting technological solutions to social problems (not hard to do); we need to know as much about security as the security services; we need to know more about communications techniques than the media, and we need to know more about networking than social-networking gurus. This knowledge can be a terrible thing, because everywhere we look we see vulnerabilities. The sad truth is that the entire edifice of modern communications is built upon fragile foundations.

It didn't have to be this way. Privacy advocates lost the argument by allowing governments and industry to define the needs of citizens and users. We would call on companies to strengthen the technical protections in their systems and they would claim that users don't care about security or are uninterested, citing 18-year-olds who want to publicise their private lives or housewives who don't want to be bothered with complex technology. We are
now facing tangible and hitherto inconceivable threats to our liberty because the entire edifice of modern communications and information technologies is built upon consumer stereotypes.

It is our collective fault now that there is a rapidly growing number of data breaches and data losses. The systems that were built to contain and protect our information are fundamentally flawed. The flow of personal data is becoming the default, and the dams erected by law are temporary annoyances for an industry interested in profiting, governments interested in monitoring and malicious parties whose motivation can be obscure. If the US State Department can’t be bothered to adequately secure its own network of inter-embassy communications, what chance is there that Facebook and Google will take better care of your personal messaging and commonly used search terms?

The irony is that the only debate we privacy advocates ever seriously won was over the right of individuals to use encryption technologies to secure their communications. We fought this battle in the 1990s, on the cusp of the information revolution, looking forward to the day when we would all have desktop computers, and everyone would use encryption technologies to secure their communications. Governments were keen to maintain their restrictions on the general public’s ability to encrypt communications so that law enforcement agencies retained unfettered access to content. We fought these restrictions and, even to our surprise, by the end of the decade we eventually won. By this time, however, governments had successfully stemmed the tide: cryptography and other privacy-enhancing technologies had come to be seen as obscure and inconvenient. Everyone is now theoretically capable of encrypting their communications – but no one does. Furthermore, restrictions on encryption remain in countries such as China, India and across the Middle East.

This is indicative of how the entire infrastructure of the modern economy and social life is built on insecurity. Privacy is becoming a popular subject, and a growing concern for the average citizen and consumer of mainstream technology. Yet users’ interest is poorly serviced.

This is why there is a frequent narrative that ‘privacy is dead’. Regardless of modern concerns, faulty decisions have been made at key moments in the development of modern computing. Microsoft was the first culprit to emphasise ease of use over security in the 1990s, leading to a decade of
annoying trojans and viruses developed by teenagers. In response, a software industry of anti-virus checkers and firewalls arose to plug in the holes so that users were informed and protected from attack. We had the chance to learn from this and make our next technological steps more informed and considered. Instead, Smartphone operating system developers like Apple and Google are now making similar mistakes by not keeping their users informed of what kind of information is leaving their devices and what applications are doing with their data. This is a repetition of Facebook’s approach when they created features that broadly shared users’ information, only later adding some features to inform users and to let them have some authority to control information flows when using third-party applications. Once your information is collected by devices and applications, as we have seen from Microsoft in the 1990s, and now Apple, Google and Facebook, it is rarely secure. In fact, your data is often readily available to any party who can query, buy, subpoena or simply steal it.

The expansion of ‘cloud’ services like Google Documents or Dropbox makes matters even worse. Instead of residing on your computers, your most confidential information is not only removed from your control, it is removed from the country and stored on foreign servers under the jurisdiction of foreign laws and law enforcement agencies. Almost universally, this information is not secured. Documents, emails and calendar information are stored in unencrypted form, and readily accessible by local law enforcement authorities.

Amongst the few positive developments, Google recently deployed disk encryption capabilities in its mobile operating system, Android, though it still has to be turned on by the user. Even when these companies do build in the capabilities for privacy, they rarely, if ever, come as standard. Security is the exception rather than the rule. After the Russian authorities began clamping down on Russian non-governmental organisations for breach of copyright (as a pretence for searching computers), Microsoft then kindly offered free versions of its operating systems to NGOs. Unfortunately, the version of Windows they offered does not include the use of disk encryption, as that is only available in the ‘premium’ editions.

At the core of this problem is companies’ perception of their typical user. The typical user in whose image applications, programs and social networks are designed is an American teenager, perfectly content to transmit and publish every detail of their personal life to an unlimited audience. It is not
the advocate, the dissident, the researcher, the professional – the people who need varying degrees of data security in order to protect their livelihoods, and sometimes their lives. Facebook, Apple, Microsoft and Google all require their users to jump through hoops in order to protect their information, and the majority of these users lack the time or awareness to do so.

In turn, companies’ systems are being probed, and vulnerabilities are being exploited. Last year, a gang in New Hampshire used ‘publicly available’ social network updates from area residents to target addresses when they knew the homeowners were out or away, stealing over US$ 100 000 worth of property in a week. A survey of hackers and security experts last year found that more than half of them were testing the limits of cloud services’ security. Meanwhile, last year a Google employee was fired after it was discovered that he was monitoring the communications of teenage girls. Far more widespread, insidious and difficult to combat than such isolated incidents of criminality are the routine surveillance practices conducted by governments. These are not techniques reserved for dictatorships. For instance, the spying capabilities embedded by Nokia Siemens in their technology for Iran’s telecommunications system, intended for the use of the Iranian authorities, were mandated by the Clinton administration under federal law applying to all US telecommunications firms, and then supported by European policy-makers and standards bodies under the more acceptable guise (or pretence) of protecting their own citizens from crime.

Some countries, like Sweden, openly acknowledge that every piece of information that enters or leaves their borders is subject to government surveillance. Whether you’re a journalist sworn to protect the names and addresses of your sources, a lawyer building a case against a corrupt highprofile politician, or a human rights advocate, all are pinning their hopes for security on a fantasy: the belief that the people who build your operating systems and applications have any way (or, indeed, any intention) of protecting you against governments who have the law on their side.

Another part of the fantasy is that governments are in control. Disturbingly, in fact, they don’t even appear to have complete mastery of their spying capabilities; for ten months during 2004-2005, the Greek government’s own surveillance technology was turned against it when an unknown adversary monitored the voice calls of dozens of government officials and cabinet members, including the prime minister. Between 1996 and 2006, Telecom
Italia had a similar breach where more than 6000 individuals’ communications were illegally monitored, for the purpose of perpetrating blackmail and bribery. As communications security expert Susan Landau noted in her testimony to the US Congress in February this year, in that period ‘no large business or political deal was ever truly private’.

Surveillance is getting easier. In the Hollywood version of governmental power, the seizure of digital evidence by the security services involves a dawn raid by armed officials, who carry off piles of hard drives, laptops and computer towers from seemingly innocuous suburban houses. This image is out of date and unrepresentative. In the 21st century, law enforcement access is just a few clicks of the mouse away. Why enter your home and read your letters when they can get into your webmail account and read every message you’ve ever sent or received? In the US, a member of staff at one of the major mobile providers recently let slip at an intelligence industry conference that the company receives eight million requests a year from domestic law enforcement agencies for specific data on geolocation; that’s a publicly traded company, one that advertises its services on billboards and TV channels across the country, not some shadowy private intelligence outfit operating under the radar.

There are companies in the business of surveillance that develop the databases, cameras, biometric scanners, DNA test kits, drones and a myriad other technologies that are being deployed around the world. Companies are also profiting from selling and buying personal information. Consider Thorpe Glenn, an Ipswich-based company that celebrates its ability to analyse the information of 50m mobile subscribers in less than a fortnight. Thorpe Glenn’s press releases boast about ‘maintaining the world’s largest social network’, with a full 700m more profiles than even Facebook can lay claim to. This practice is rapidly becoming an industry.

Chris Soghoian, a researcher in the US, has found that companies frequently get paid for each instance they respond to government requests. Google, for example, has received US$25 for responding to a request for data from the US Marshal Service. Yahoo!’s ‘Cost Reimbursement Policy’ offers US$20 dollars for the first basic subscriber record and then a discounted US$10 per ID thereafter, though email content is US$30-$40 per user. They could, technically, develop a business model just on handing over information to law enforcement agencies. Jokes aside, what incentive do these providers have to make communications infrastructure more secure? There are,
however, some signs of change. Over the past year some companies have announced security and privacy advances in their products and services. Certainly the uprisings across the Arab world helped, as companies did not want to be seen on the wrong side of history and face the same kind of admonishment as Nokia Siemens after the Iranian elections in 2009. Google vacillated for years before turning on encryption on its network layer, but it is swiftly becoming common practice. It is to be hoped that we will see a similar paradigm shift now that Facebook has enabled users to turn on HTTPS to help protect data as it passes through the internet (although predictably enough it has yet to employ HTTPS by default, making it less easy for people to use it). The global struggles against abusive governments have also focused international attention on the enormous capacities of those governments to spy on their citizens, and the enormous human cost of this kind of all-pervasive surveillance. Once the behemoths of the internet take positive steps, smaller companies will hopefully follow.

Yet so long as the key technology developers keep on assuming that their users are uninterested, and so long as they seek to profit by selling our habits and interests, we will all remain vulnerable. It is now time for a mature policy debate on privacy and security. Not one that sees the benefit of the state as paramount, nor one that presumes that if a service is free then the user’s information can be exploited. Business models should fail with each security and privacy blunder, just as laws should be called into question with every new breach and abuse. The rise of mobile devices and cloud services is a replay of the 1990s all over again, where the policy and business world is grappling with technological change and telecommunications growth. If left to their own devices, governments will build more vulnerabilities and back doors while industry will acquiesce and build for ‘sharing’ and ‘organising the world’s information’. If we can hold on to this moment in history just a bit longer, and keep these companies thinking about the global community of diverse users, and not merely those who are 18 years old, while reminding them that backdoors aren’t always used for noble purposes, then we may have a fighting chance. Perhaps we can even chalk up a real win this time.