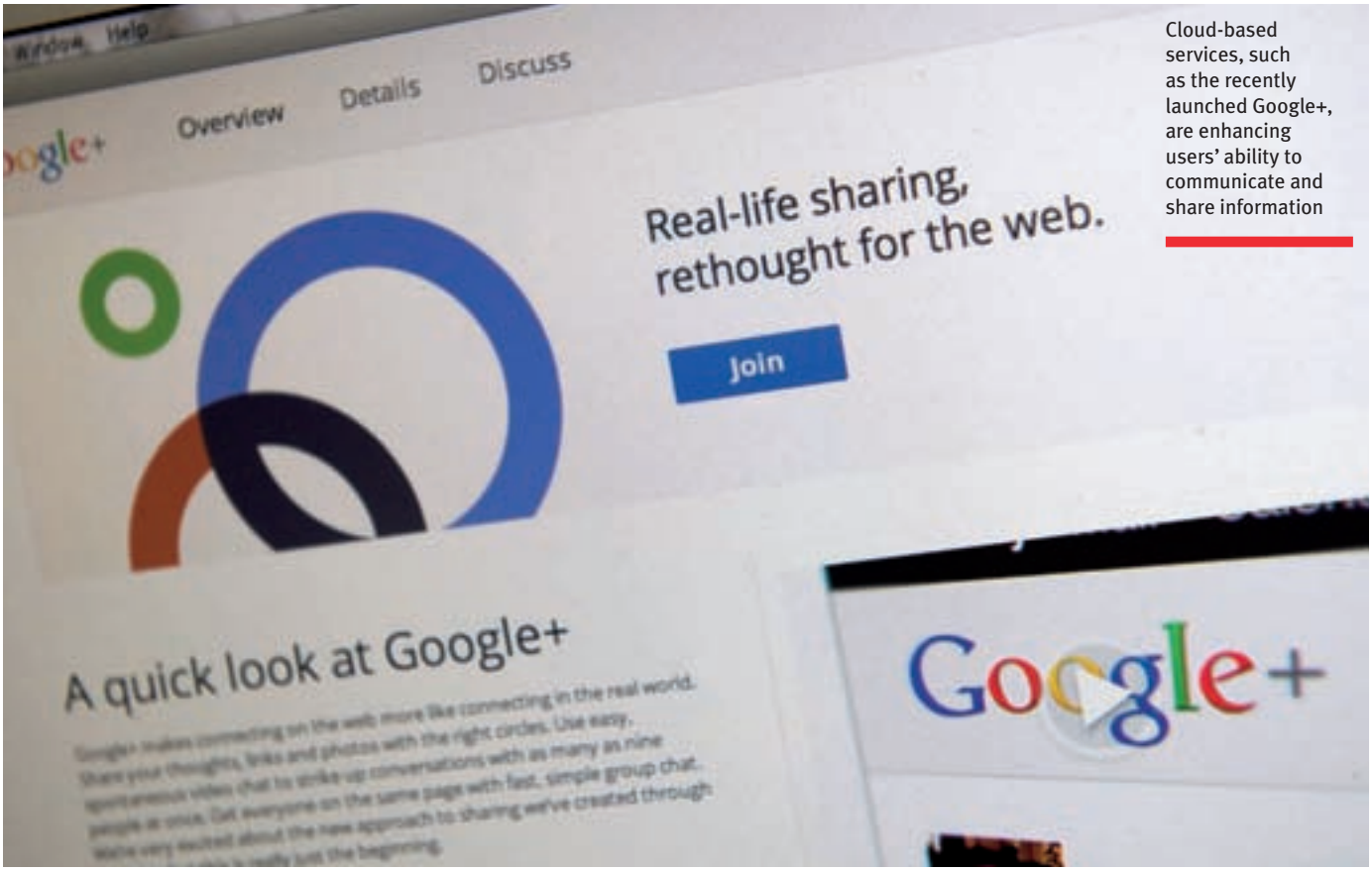

Cloud-based services, such as the recently launched Google+, are enhancing users' ability to communicate and share information

Questions of trust as we head into the 'cloud'

As growing numbers of internet users migrate their data from their own devices to the servers of 'cloud-computing' providers, issues of policing, privacy and human rights are coming to the fore, not least in states where democracy is lacking

By Ronald Deibert, director, Canada Centre for Global Security Studies, Citizen Lab, Munk School of Global Affairs, University of Toronto

Though barely noticeable, a major tectonic shift has happened in global communications. Data previously stored only on desktops, on hard drives and in filing cabinets has evaporated into the 'clouds'.

'Cloud computing' refers to the delivery of software and other services as a utility over computer networks. But the cloud has become a metaphor for the way today's digital lives have been dispersed into a globally distributed mist.

Whereas, before, the internet was a self-segmented network distinct from other means of communication, such as television, telephony and radio, all these media have become integrated into a single system of planetary communications called cyberspace. This has happened at the same time as business models and service-delivery mechanisms for information and communications have changed fundamentally, with the rise of social networking, mobile connectivity and cloud computing (referred to together here as the 'cloud').

For large organisations, such as businesses and governments, the cloud provides a major cost-cutting solution. For individuals, it is convenient, reliable and fun. For the companies that support the cloud and the various products, services and devices that connect to it, it is an attractive source of growing revenue and innovation.

But there are dark sides. The shift to the cloud represents a paradigm shift in communications, which has upset the principles, norms and rules of what used to be just the internet. Under the internet's operating paradigm, the companies that ran the infrastructure took a 'hands-off' approach to the content that flowed through their networks, a principle known as 'network neutrality'. Today, data is entrusted to vast transnational information

empires – such as Google, Facebook and Amazon – that act as gatekeepers of what gets communicated and what is accessible. Market considerations can easily outweigh privacy and other rights concerns.

The rapid shift to an entirely new ecosystem has also opened up unforeseen insecurities that are systematically harvested by opportunistic actors, including criminals, unethical businesses, and military and intelligence agencies. Whereas at one time people's data was only as secure as they could protect it behind closed doors in their offices and filing cabinets, today it is only as secure as the companies that host it. In principle, entrusting data to third parties should actually enhance security because security is delegated to professionals that should have the ability to keep up with the latest threats. But studies have shown that cloud-computing companies are far less concerned with security than the bottom line. Some spend less than 10 per cent of their information technology resources on security.

Not surprisingly, there has been a growing rash of major security breaches across governments and the private sector. According to Privacy Rights Clearinghouse, nearly 600 million records have been breached due to the roughly 2,670 data breaches made public since 2005, in the United States alone. Included among these was the breach of Epsilon systems, resulting in a loss of more than 60 million email addresses from more than 50 companies. A breach of Sony servers in April 2011 resulted in the exposure of the private data of more than 100 million people. Major US defence contractors have also now admitted to persistent breaches and attacks.

Although many of these breaches appear to be mostly opportunistic hacks by anti-authoritarian groups intending to wreak havoc against 'the system', a growing number have sophisticated political and economic motivations. Research by Citizen Lab and the SecDev Group has uncovered cloud-based espionage networks emanating from Chinese, Iranian, Syrian, Burmese and other national jurisdictions pursuing numerous high-profile government, military, political, opposition and human-rights targets across Asia, Europe and North America.

One overarching characteristic is that the trade craft employed by the perpetrators is usually indistinguishable from that used in the ecosystem of cybercrime. As cyberspace becomes an object of geopolitical contests and a political battlefield among authoritarian regimes and their adversaries, clouds will become vectors for cyber-espionage and politically motivated attacks.

Transcending jurisdictions

The shift to the cloud has also created new governance issues. While the notion of the cloud may seem ephemeral and be experienced by users as a virtual mirage, the infrastructure in which it is embedded involves a complex material, logistical and regulatory infrastructure that can span multiple political jurisdictions, from the local to the national to the international. While the text, the image and the video all may still seem within our immediate grasp, on our desktops and handheld devices, they are not. Data that we handle – that we assume is in our possession – is transported in an instant over cables and through radio waves from arrays of servers, many of which are far away in another political jurisdiction. And almost all of it is owned and operated by the private sector.

Governments looking to control cyberspace must therefore enlist the private sector that owns and operates the cloud to 'police the internet', through laws, regulations, incentives or other types of pressures. For example, in Canada, the government has introduced a crime bill that would require internet service providers (ISPs) and telecoms companies to retain user data, process the data for law enforcement and intelligence consumption, and share it with law enforcement representatives – all without judicial oversight. Such arrangements are not uncommon. Telecom carriers and ISPs not only facilitate access to information for law enforcement, but also actually derive revenues from doing so, and there is extensive variation among them on how exactly they go about doing so. As a result, citizens using different communications services can live in entirely different universes of rights.

The downloading of policing functions to the private sector – a phenomenon known as 'intermediary liability' – extends to the protection of intellectual property. It is considered standard practice for large carriers to 'clean their pipes' of malicious networks and traffic associated with file sharing or other activities deemed copyright-infringing. In the United States, several ISPs and carriers have already taken on this responsibility as a voluntary arrangement. The bottom line of business now demands it.

Manipulation by non-democratic states

Of course, what is considered intermediary liability or a market imperative in Canada and the United States differs quite fundamentally from the situation in Belarus, Iran, Vietnam or China. In non-democratic countries, ISPs, telecom carriers and mobile operators are asked to police political content, track dissidents, identify protestors, send threatening messages over their networks and disable certain protocols used by adversaries – as part of the next-generation controls emerging in cyberspace. During the Arab Spring, for example, the Egyptian government forced ISPs to shutter the internet and required the country's main mobile phone operator, Vodafone, to send mass text messages encouraging pro-regime sympathisers to take to the streets to counter the protestors.

Citizens can find themselves hamstrung in jurisdictional confusion. When the US-based son of an Iranian activist, arrested presumably after his cell phone records were turned over to Iranian authorities by his provider, filed a lawsuit against Nokia-Siemens in an American court, the company argued that it was the wrong case in the wrong jurisdiction, and that it was merely following local law. The suit was eventually withdrawn.

In Canada, the Rogers Yahoo! internet privacy policy states that "personal information collected for the Internet Service may be stored and processed in Canada, the United States or other countries and may be subject to the legal jurisdiction of these countries". Users might well ask which countries and whose laws. As people's data evaporates into the clouds, so seemingly do their rights.

The trend towards the clouds may be irreversible, but its direction can be shaped in ways that mitigate some of its more serious dark sides. The private sector that owns and operates the clouds should be required to spend as much, if not more, effort protecting users' privacy and data as it does policing the internet for law-enforcement and intelligence agencies and copyright holders. If market forces are not enough, data-breach and privacy-by-design laws should be introduced, both domestically and through global cyber-security forums. Civil-society networks, including university researchers, play an important role as well, monitoring the private sector, uncovering and exposing security flaws and other forms of corporate negligence, and educating users on best practices.

More broadly, there needs to be a reinvigorated discussion of what public transparency and accountability mean as data levitates to the clouds and private authority in cyberspace becomes the norm. There is an urgent need to strengthen the protections against when data can be shared with third parties without users' knowledge or permission. Private forms of authority should be subject to the same type of rigorous checks and balances as is public authority, especially as their operations can span political borders where rights protections diminish. Until such time, dark clouds will continue to grow more ominous on the horizon, threatening to diminish human rights. ◆

"As cyberspace becomes an object of geopolitical contests, clouds will become vectors for cyber-espionage and politically motivated attacks"