Who owns the Internet?

Dr Victoria Baines, IT Livery Company Professor of IT

20th September 2022

"Who owns the Internet?" It's a very simple question until one tries to answer it.

And it prompts further questions, not least among them, "What exactly *is* the Internet?" For thousands of years, describing and defining property has helped us decide to whom it belongs. Physical extent and location have traditionally enabled societies to determine not only the rightful owner, but also the country under whose jurisdiction something falls.

This principle of state sovereignty, which is at least as old as the 1648 Peace of Westphalia between major European powers, bestows on governments control and oversight of whatever takes place on their territories. As enshrined in Article 2 of the United Nations Charter, it protects sovereign nations from "the threat or use of force against the territorial integrity or political independence of any state."

Indeed, territory is the very basis of modern sovereignty, jurisdiction, and diplomacy. The advent of the Internet challenges this territorial approach. If we choose to define the Internet as its infrastructure, hardware, data centres and exchange points, it is possible to pinpoint their locations and the countries under whose jurisdiction they fall. But the Internet is also cyberspace, billions of connections and pieces of content created by all of us. As such, it resists the attempts of governments to control what their citizens see and do on it. Indeed, freedom from territory and therefore from ownership is central to collaborative, consensus-based models of Internet and cyberspace governance, of which Internet pioneer John Perry Barlow's (1996) *A Declaration of the Independence of Cyberspace* is perhaps the best known [emphasis added]:

> *"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us.* ***You have no sovereignty where we gather****.*
>
> *We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear."*

Barlow highlights not only the ideological arguments against simply imposing government control on cyberspace, but also the practical challenges of doing so [emphasis added]:

> *"Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.*
>
> ***Your legal concepts of property****, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here."*

In many countries, ownership of Internet infrastructure is in private hands, among them domestic Internet service providers (ISPs) and multi-national corporations. Increasingly, technology companies such as Microsoft and entrepreneurs such as Elon Musk seek to shape society's future through direction of its information and communications technology. As of summer 2022, Musk reportedly owns one third of all the

active satellites in Earth's orbit and plans to increase this proportion to two thirds by the autumn of 2023.[1] His decision to supply Ukraine with satellite-based communications equipment has been widely credited with keeping the country's Internet access up and running following Russia's invasion. In this respect, Big Tech executives have become leading players on the world stage, statesmen in their own right, whether governments like it or not.

This hasn't stopped governments trying to control the parts of the Internet they deem to be on their territories and within their jurisdictions. In countries with state-owned or state-controlled ISPs, it is arguably easier to restrict who can access the global Internet (as in the case of North Korea), and which platforms are accessible to citizens (China, Iran, and Russia being the best known examples of these). But even in countries with evidently freer societies, governments seek to police the information accessible to their citizens online.

Where more oppressive regimes tend towards information control in the interests of national security, public order, and morality, Western democracies ostensibly focus on removing content that may harm individuals or pose a risk to their safety. The motivations may vary, but without exception governments seek to influence what their citizens see on the Internet. We can find evidence of this in the transparency reports published by the largest US tech companies. For example, these are the top ten countries who in 2021 requested that Meta (formerly Facebook) restrict content on its platforms:[2]

Requesting Country	Content Restriction Requests to Meta
Mexico	20,568
Germany	16,214
Argentina	9,098
Taiwan	5,646
Pakistan	5,600
Indonesia	4,038
Russia	3,099
Brazil	2,910
United Kingdom	2,645
Thailand	2,643

Fig. 1 Top Ten Countries sending content restriction requests to Meta in 2021 [Data source: transparency.fb.com]

It's immediately apparent from the list above that countries requesting the largest number of restrictions do not conform to a particular type. Meta's reporting also reveals that these countries have different ideas of what should be removed from social media. Mexico and the UK are notable for their focus on consumer protection and advertising standards, Pakistan and Indonesia for restrictions of blasphemous content, Russia for restriction of separatism and extremism, content deemed to be in contravention of the 'patriotic education of young people', and content related to the invasion of Ukraine. But all of these countries make several thousand requests a year to render content on the Internet inaccessible to their citizens. This is technically possible because for the most part our connected devices can be 'geo-located' to a country by their Internet Protocol (IP) addresses. Countries notably absent from Meta's data have other means to restrict content: China by blocking access to sites deemed to contain politically sensitive keywords – the so-called Great Firewall of China; the US by virtue of the fact that the operations of Silicon Valley companies are governed primarily by US legislation. Their terms of service – the rules users agree to abide by when they sign up – are rooted in US notions of acceptable behaviour and content.

This in turn prompts another key question, "Who should protect you on the Internet?" The Westphalian world order prescribes that sovereign states are responsible for protecting their citizens and maintaining public safety. According to political philosophers Thomas Hobbes, John Locke, and Jean-Jacques Rousseau, there

[1] https://edition.cnn.com/2021/02/11/tech/spacex-starlink-satellites-1000-scn/index.html; https://interestingengineering.com/innovation/starlink-to-double-satellites

[2] You can examine this data for yourself at https://transparency.fb.com/data/content-restrictions/global/

is a social contract between governments and citizens, the terms of which include a duty of governments to protect citizens, and the right of citizens to that protection in exchange for some of their freedoms. But since so much of the Internet is in private ownership, the private sector clearly has some responsibility for our safety and security. This responsibility to protect extends also to responding when something goes wrong. When we are physically assaulted by someone, or when someone steals our physical property, we typically appeal to the police and the criminal justice system to hold the offenders to account. When we are victims of online crimes, we likewise expect someone to do something about it, but the burden of that responsibility appears to be shared between the police and the online platforms and providers. This is borne out by the results of a poll YouGov conducted for us on a representative sample of UK adults.[3]

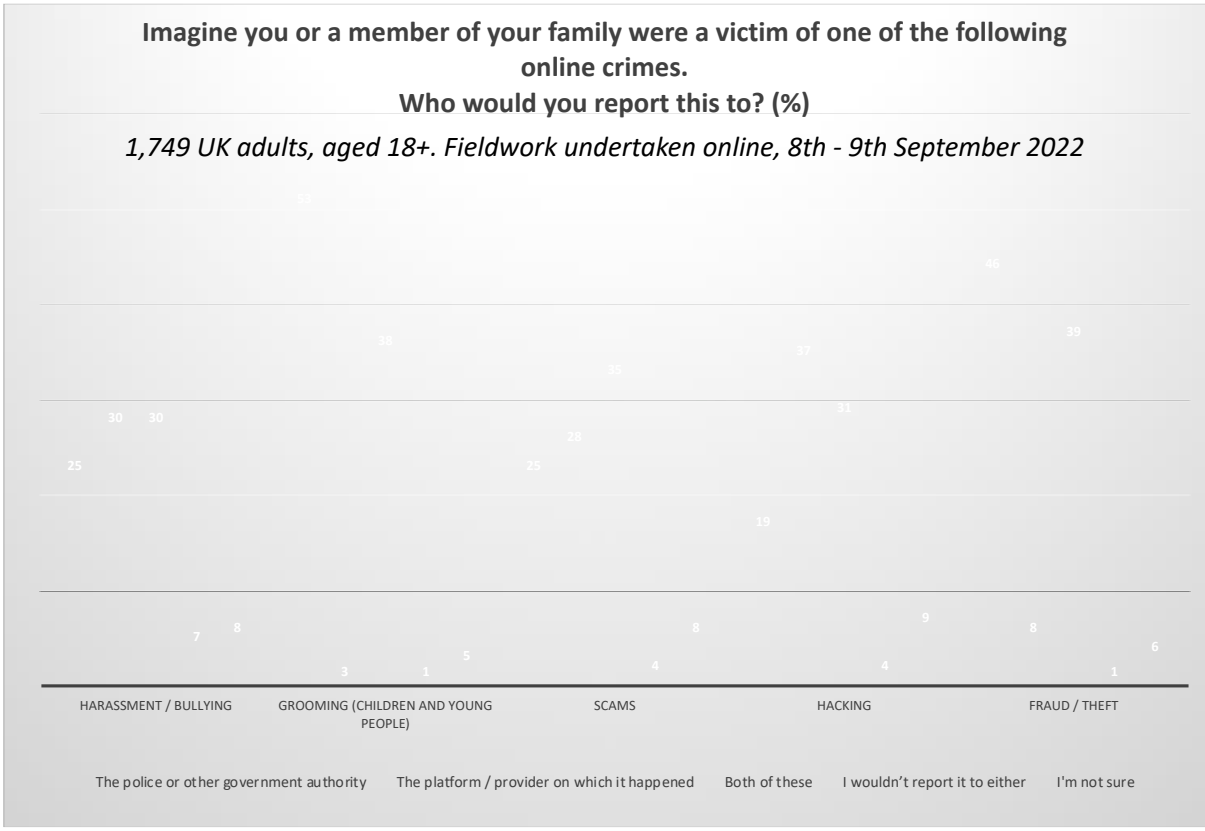

Fig. 2 YouGov poll of UK adult sample on reporting of online crimes

The good news is that the vast majority of people - an average of 89% across the five crime types - said that they would report to someone, whether the police, the platform on which the crime occurred, or both. For grooming of children and young people and fraud or theft, people were most likely to contact only the police. But for hacking, respondents said that they were most likely to contact the platform alone. When we factor in those people who said that they would report to both the police and the platform, we find that in total just 50% would report hacking to the police, and 55% online harassment. While this is a relatively small sample of 1749 people, it indicates that, at least for some crimes, people now look to tech companies for the first response traditionally provided by the police.

Just as road safety requires a whole society response, so too with the Internet. We rightly don't put the responsibility for preventing road traffic accidents solely on the automotive industry. Likewise, all the technical safeguards in the world can't eliminate the impact of human error or criminal intent on the Internet, nor should we expect them to. At the same time, ongoing negotiations between states – for example, in the United Nations for a new international cybercrime treaty – reveal familiar national preoccupations with sovereignty, particularly information and access control, and run the risk of casting cyberspace as a battleground rather

[3] All figures, unless otherwise stated, are from YouGov Plc. Total sample size was 1,749 adults. Fieldwork was undertaken between 8th and 9th September 2022. The survey was carried out online. The figures have been weighted and are representative of all UK adults (aged 18+).

than a common heritage of humanity. What are the alternatives?

Following existing models for managing the Internet's architecture, a number of multi-stakeholder frameworks for cyberspace governance have been proposed. Among these are the principles promoted by the Global Commission on the Stability of Cyberspace, an international group of senior level cyber experts jointly sponsored by governments, multi-national corporations and civil society organisations. The Commission advocates:

- Responsibility: Everyone is responsible for ensuring the stability of cyberspace.
- Restraint: No state or non-state actor should take actions that impair the stability of cyberspace.
- Requirement to Act: State or non-state actors should take reasonable and appropriate steps to ensure the stability of cyberspace.
- Respect for Human Rights: Efforts to ensure the stability of cyberspace must respect human rights and the rule of law.

This community approach envisages 'everyone' as all citizens of the world, not only the powers that be: specifically, "every individual connected to cyberspace must take reasonable efforts to ensure their own devices are not compromised and, perhaps, used in attacks." Challenging the long-held notion that governments secure public spaces on our behalf, it demands more of us as citizens of cyberspace. It gives us responsibilities as well as rights.

Time will tell whether the proposals of the Global Commission are anything more than a thought experiment. They nevertheless give us a glimpse of the direction in which Internet and cyberspace governance could head if states are willing to take a more inclusive – and arguably realistic – view of who owns the Internet and who has a responsibility to protect it. What is already evident is that governments cannot keep this contested space safe, secure, or stable without the help of private companies, and decisions about how it should be governed should benefit from the input of informed citizens. The Internet is too important to all of us to be a puzzle solely for programmers, police, and politicians.

Have Your Say, Own the Internet

Have your say on the two key questions of this lecture:

1. *Who owns the Internet?*
2. *Who should protect people on the Internet?*

Go to Slido.com to register your answers: https://app.sli.do/event/7urr6Rnnrh2VccHy5vx5T6

We will include the results in a published article on the role of citizens in cyberspace governance. Your opinion matters, so **please do vote**!

Resources

The Internet Corporation for Assigned Names and Numbers (ICANN) is the non-profit organisation responsible for managing the global system of web domain names and addresses. Its website features a *Beginner's Guide to ICANN*, which includes an online learning platform on Internet governance and information on regional events. https://www.icann.org/get-started

You can also follow the work of the United Nations' Internet Governance Forum (IGF) for the latest discussions on Internet governance and global ICT policy. https://www.intgovforum.org/en/about#get-started

Further Reading

Barlow, J. P. 1996. *A declaration of the independence of cyberspace*. https://www.eff.org/cyberspace-independence

Global Commission on the Stability of Cyberspace. 2019. *Advancing Cyberstability: Final Report November 2019*. The Hague. https://cyberstability.org/report/

Internet Engineering Task Force. 1996. *Architectural Principles of the Internet*. https://datatracker.ietf.org/doc/html/rfc1958

Smith, B. 2022. *Defending Ukraine: Early Lessons from the Cyber War*. Microsoft On the Issues Jun 22, 2022.

https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

Data and Visuals

Meta. *Content restrictions based on local law.* https://transparency.fb.com/data/content-restrictions/global/

The Opte Project. *The Internet 1997 – 2021*. https://www.opte.org/the-internet

Bazzan, Colombo, Giordano, Misto, Piro & Stosjic. *The Physical Internet*. https://densitydesign.github.io/teaching-dd15/course-results/es01/group04/

Telegeography. *Submarine Cable Map.* https://www.submarinecablemap.com/