# The Role of Government

As the Internet becomes more deeply embedded into every aspect of our lives, governments will to play a far more active role in ways that will impact the economy, civil rights, freedoms and the Internet itself.

## Overview

As the Internet expands further into our economy and society, governments will be even more active, both as policymakers and as Internet users themselves. From cybersecurity to societal issues to technologies such as the Internet of Things (IoT) and Artificial Intelligence (AI), governments will face a host of new and complex issues that will challenge all aspects of their decision-making. Technology will increasingly influence the relationship between governments and other stakeholders. As public services and data collection shift to private companies, the roles of the public and private sectors will continue to blur, complicating how citizens hold governments to account. How governments respond to these challenges in the future will impact not only our freedoms, rights and the economy, but also the Internet itself.

Internationally, cybersecurity will drive global governance discussions for the foreseeable future, with the growing risk that governments will limit freedoms or undermine the global nature of the Internet. The Internet will not be immune to the evolving geopolitical tensions driven by nationalism, multilateralism and global power dynamics. How and if states resolve these tensions in the coming years will have tangible implications for the global reach of the technology as well as the overall growth of the Internet economy. To the extent that international cooperation continues in the Internet space, we expect that the tension between multi-stakeholder and multilateral[1] approaches to Internet policy will continue.

**The future of Internet openness will depend on how governments deal with the growing pressure to respond to security challenges.**

**New technologies and game-changing business models will force governments to work differently and more inclusively.**

**Roles and responsibilities in the public and private sectors will continue to blur, creating accountability challenges.**

**Government policies and structures will be ill-equipped to keep pace with technological developments.**

**Nationalistic policies will endanger valuable cross border data flows, trigger fragmentation of the network, and silence critical stakeholders.**

[1] In multistakeholder processes, individuals and organisations (stakeholders) from different realms participate alongside each other to share ideas or develop consensus policy. In multilateral systems, several countries and governments work together to solve a particular problem or reach a shared goal.

## Government Responses to Future Security Challenges

The scope and complexity of cyberattacks will continue to intensify. Governments will face mounting pressure to act forcefully to protect national security, their citizens and their domestic economies. In fact, our community believes that we are facing a future of increased Internet regulation or legislation.[2]

Yet, policymaking that is reactive and not long term may further fragment the Internet along nation-state boundaries, and also undermine human rights. As the Internet expands into every sector of the economy, the sheer complexity of the security landscape will test even the most sophisticated governments' coordination, capacity and effectiveness. The challenge for developing countries will be even more acute: while Internet Society stakeholders in Africa are confident that their governments see the cybersecurity challenge, they are concerned that governments will lack the skills and capacity to tackle the issues effectively.

> **Respondents from North America predicted future government reactions to the security challenge to be significantly more drastic than their counterparts in Africa, Asia, and Latin America.[3]**

There is a trend today for governments to demand more control over Internet content within their borders in ways that undermine Internet openness, compromise freedoms and rights, and threaten global Internet fragmentation.[4] This could happen in several ways.[5]

Technically, fragmentation will happen if limits are put on the ability of the system to fully interoperate and exchange data packets in an end-to-end way. Governmental fragmentation will happen if states put measures in place that hinder the global reach of the Internet. This scenario could become a reality if governments prioritise short-term national interests — sometimes referred to as "cyber sovereignty" — over longer-term interests and shared responsibility.

[2] Future of the Internet Survey 2 - Question 26: "To what degree do governments regulate or pass laws regarding the Internet"?
[3] Future of the Internet Survey 2 - Question 31: "How extreme are government responses to security risks, challenges, and crises involving the Internet"?
[4] https://www.schneier.com/blog/archives/2013/03/nationalism_on.html
[5] Internet Fragmentation, An Overview, WEF

# The Role of Government

**Our community believes that government regulations of the future will be more intrusive and restrictive than today.**[6]

How governments respond to security challenges will either strengthen people's trust in the Internet or undermine it. In an age of cyberattacks and even cyberwar, some policy makers will sacrifice freedoms and innovation in the name of national security and public order.

> "The most pessimistic scenario for the future of the global Internet is fragmentation due to nationalistic isolation with highly-filtered access to the Internet.
>
> Technologist, North America

The tension will continue between the need to secure communication for economic and privacy reasons — and governments' need to access those communications for national security. If governments persist in trying to prevent the use of encryption, they put at risk not only freedom of expression, privacy, and user trust, but the future Internet economy as well. Further, interfering with or weakening encryption technologies will create new vulnerabilities and cyber threats.

**Our community believes there will be a high degree of acceptance of encryption in the future.**[7]

> "My worst fear is a surveillance state making 1984 resemble a utopia or a glorified cable TV subscription service. One where encryption is banished, anonymous access to the Internet is legally/technically eliminated and the censorship slippery slope continues.
>
> Technical Community, Europe

> "Nationalism and extremism are shaping the Internet but their influence is disproportionate to the space they occupy.
>
> Civil Society, Middle East

> "Political views will be expressed more readily online than the traditional way of going out on the streets. Democracy of communications will culminate in greater transparency and accountability of governments.
>
> Government, Africa

> "Governmental interest in national security will continue to manifest in regulatory actions which inevitably compromise personal privacy and security.
>
> Technologist, Asia-Pacific

Related to: Cyber Threats; Personal Freedoms & Rights

[6] Future of the Internet Survey 2 - Question 27: "How intrusive or restrictive are government regulations or laws on Internet use, services, or operations"?
[7] Future of the Internet Survey 2 - Question 23: "To what degree is the use of encryption and cryptographic technologies on the Internet accepted by society"?

## Policy Making in the Digital Age

The sharing of citizens' data between the public and private sectors will continue to grow, as will the blurring of roles and responsibilities between the public and private sectors as the delivery of public services shifts to the private sector. Could this result in the private sector assuming responsibilities that are traditionally those of governments'? If so, will they be subject to the same accountability and governance mechanisms as governments? In the future Internet economy, the use of IoT and artificial intelligence will increase the need to be vigilant about transparency and accountability in decision-making and governance. Transparency and accountability will also be needed to understand and manage an increasingly complicated relationship between the public and private sectors.

> "The private sector is displacing governments as the locus of policymaking — including in the enjoyment of human rights.
>
> Civil Society, North America

Although cybersecurity concerns will continue to be front and centre, governments will also grapple with IoT and AI. In the face of new technologies, are the existing policy tools able to address the complexity of the challenges ahead? According to our community, policymakers will struggle to keep pace with change in Internet technology in the future.[8]

> "Technology advances more rapidly than policy and the regulatory environment.
>
> Government, Africa

> "The speed at which legislation and regulatory frameworks that affects the Internet services can be modified, is an anachronism compared to the technological changes.
>
> Government, Latin America & Caribbean

There will be more pressure on governments to act, even as society struggles to keep up with the pace of change, let alone to consider the long-term implications of today's choices. Governments need to prepare for dramatic changes in the economy, especially in traditional industries most challenged by technology. Government's tendency to apply legacy regulatory models to new and emerging issues is of particular concern.

Whether or not governments chose to take such an approach, the scope of market change driven by dramatic advances in technology will inevitably force a fundamental rethink of existing approaches in competition law and traditional communications regulation. Data will increasingly be seen as an asset linked to competitive advantage, changing the nature of merger reviews, evaluations of dominance and, importantly, consumer protection.

**Respondents from Africa predict the greatest increase in regulation.**[9]

Governments may turn to multi-stakeholder models of policy development out of necessity, as traditional telecommunications and Internet regulatory approaches are longer seen as fit for purpose.

Related to: The Internet Economy; Personal Freedoms & Rights; The Internet & the Physical World; Artificial Intelligence

[8] Future of the Internet Survey 2 - Question 28: "How intrusive or restrictive are government regulations or laws on Internet use, services or operations"?
[9] Future of the Internet Survey 2 - Question 26: "To what degree do governments regulate or pass laws regarding the Internet"?

## Multistakeholderism and Multilateralism and the setting of global norms

Will governments embrace globalisation, or will they respond to domestic pressures to strengthen both physical and cyber borders? Will they support and promote multistakeholder approaches to policy, or will they retrench behind the walls of multilateralism? The rise of nationalism and populism around the globe could cause governments build national policy barriers that fragment the Internet. If current trends are any indication, more and more governments will restrict and control Internet use and access through censorship, network shutdowns and other means.[10]

> **All stakeholder groups and regions saw significant policy and regulatory differences between nations today; however, respondents also saw a trend toward global compatibility — although they were uncertain about the final outcome.[11]**

At the same time, governments could become more attuned to the need for cross-border and cross-sector cooperation on cyber threats like crime and terrorism. The complexity of the challenges should compel governments to work with other stakeholders.

[10] https://freedomhouse.org/report/freedom-net/freedom-net-2016
[11] Future of the Internet Survey 2 - Question 25: "Are national Internet policies and regulatory frameworks globally compatible or are there strong differences along national or regional lines"?

However, for such efforts to work and to have legitimacy, they will need to move beyond traditional public-private partnerships and include civil society.

Multistakeholder approaches will continue to receive measured support from *some* governments, particularly when it comes to setting norms and best practices for cyberspace. But political change is slow, and the tension between multilateralism and multistakeholderism will continue for the foreseeable future.

> “
>
> The legal tools available to address cyberattacks have limited teeth and lack the ability to prosecute. There will be a need to review existing laws to strengthen the legal framework in dealing with emerging cybercrimes.
>
> Technologist, Latin America & Caribbean

> “
>
> Fragmentation of the Internet will occur without coordination of multistakeholder and governance mechanisms.
>
> Technologist, Latin America & Caribbean

While our community is optimistic, predicting more use of multi-stakeholder approaches in the future,[12] they also question whether civil society groups and activists will have a real seat at the table. The answer to this question will have significant implications for the future of online rights and freedoms.

> “
>
> It is essential to radically strengthen users and civil society powers in the multistakeholder model to compensate for the relative decline of direct governmental influence.
>
> Government, Europe

Will we see new models of Internet governance in an evolving multipolar world? How will these diverging models and the rise of new powers shape the global Internet and its core principles? If the international system continues to turn inwards, the implications for the *global* Internet will become ever more profound.

> “
>
> I am concerned with an increased consolidation in businesses, government positions and Internet governance resulting in alliances to preserve the status quo.
>
> Technologist, Latin America & Caribbean

Related to: The Internet Economy; Cyber Threats; Networks, Standards & Interoperability

[12] Future of the Internet Survey 2 - Question 29: “Are major decisions on Internet governance and policy made primarily through multistakeholder approaches or more strongly by national governments or multilateral approaches”?