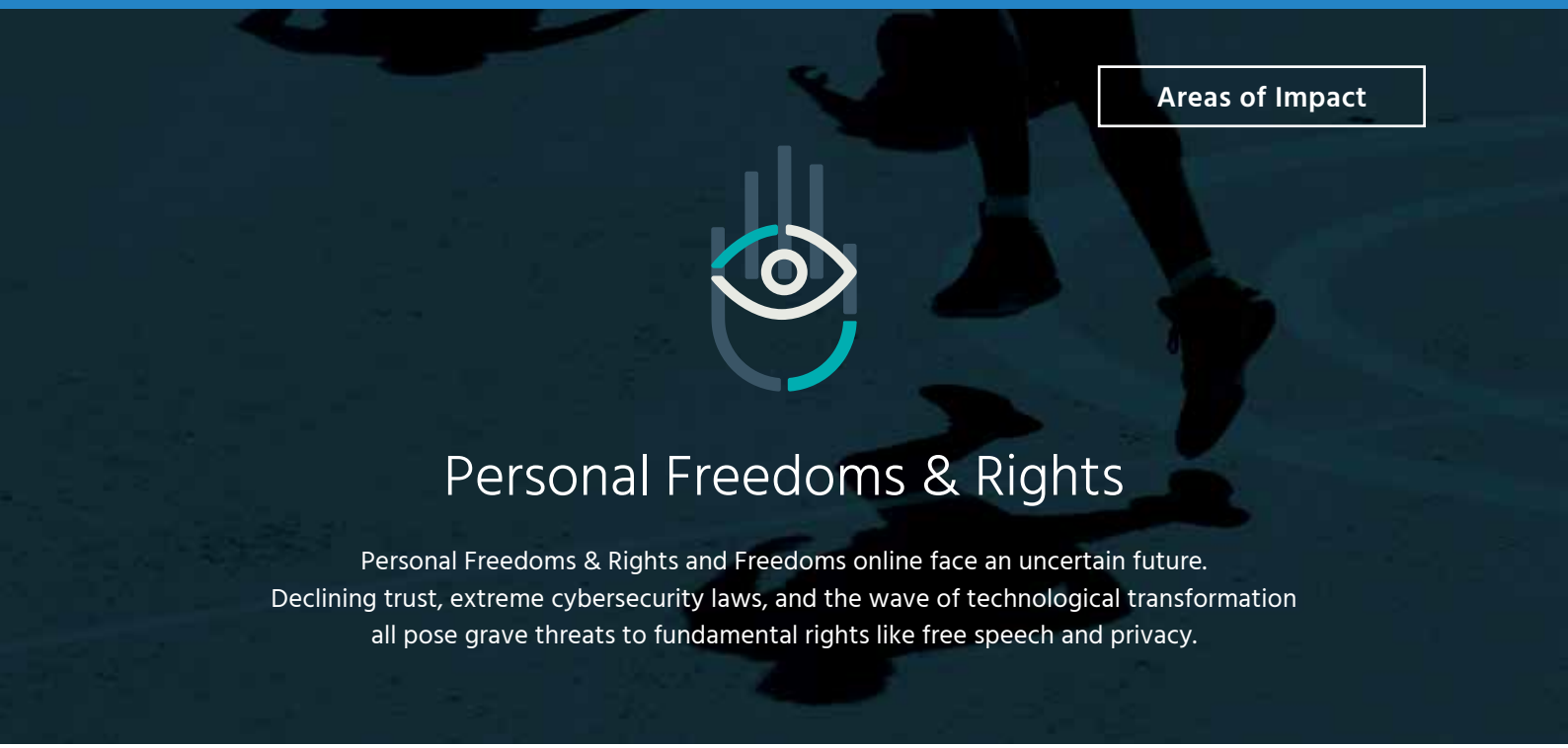

Personal Freedoms & Rights

Personal Freedoms & Rights and Freedoms online face an uncertain future. Declining trust, extreme cybersecurity laws, and the wave of technological transformation all pose grave threats to fundamental rights like free speech and privacy.

As the scope and severity of cyber threats intensifies, and as global Internet platforms are used to deliberately spread disinformation, users will lose trust in the Internet.

If aligned with human interests, advancements in technology will change the lives of people all across the globe by making the delivery of critical services more efficient and by transforming education, healthcare, and many other aspects of the economy and society.

Advanced deployments of AI & IoT will result in the generation and collection of enormous amounts of information about individuals that can be analysed in ways that are deeply personal and that will raise the potential for a "surveillance society" to emerge.

All governments are under increasing political, economic and social pressure to respond to cyber threats, terrorism and violent behaviour online. Measures that may be intended to secure cyberspace will increasingly undermine Personal Freedoms & Rights.

Overview

For many, the growth and ubiquity of the Internet is a sign of progress and innovation. They see the Internet as an enabler of human rights such as free expression, free association, and social empowerment. The Internet allows people to create and join new communities and eliminates geographical barriers to making connections. Younger users and those in developing countries are particularly optimistic about the future of the Internet and the ability to use the technology to better their lives and create their futures. And yet, many in our community are worried that the future will see greater challenges to core Internet rights like privacy and free expression.

The future of the Internet is inextricably tied to people's ability to trust it as a means to improve society, empower individuals and enable the enjoyment of human rights and freedoms.

Powerful Internet-enabled data analytics and artificial intelligence will raise important questions about the future of personal autonomy and decision-making and a lack of transparency may undermine user trust. As the scope and severity of cyber threats continues to grow, governments will put stronger measures in place, often in the name of national security, that will impact personal freedom and human rights. We already see a decline in Internet freedom across the globe and we fear that, without a change of course, personal freedoms and rights online may well be nearing a point of irreversible decline.

The Loss of Trust in the Internet

Ultimately, the power of the Internet hinges on users' willingness to trust it. They must trust that their data is secure, that their interactions will be respected, and that their expectations of privacy will be met, among other things. Unfortunately, current trends tell us that trust in the Internet is on the decline, in large measure due to the rising numbers and types of cyber threats and concerns about fake news and disinformation.

The 2017 CIGI/IPSOS study revealed that: "A majority of global citizens are more concerned about their online privacy compared to a year ago".[1] People in the developed economies said they were losing their trust in the Internet because they are worried about "government behaviours and control by corporate elites". Similarly, respondents to a recent Internet Society survey in Asia Pacific listed cybersecurity, data protection and privacy among the top five Internet policy concerns for the region[2]. And there are broader implications for development, with one member of our community suggesting that "access will not be achieved as hoped if trust is not addressed". Having said all this, Internet usage in general continues to rise, social media remains popular, and the sharing economy shows no signs of slowing down.

> "Lacking progress, the Internet risks losing "simple", "honest" people to trolls, spammers and malware. Commerce could collapse on the internet due to a lack of trust and effective legal recourse.
>
> Technologist, Europe

[1] https://www.cigionline.org/internet-survey
[2] https://www.internetsociety.org/news/cyber-security-tops-list-concerns-internet-users-asia-pacific

Personal Freedoms & Rights

Internet users fear that they will be on their own when it comes to managing their online security and the never-ending parade of data breach announcements by industry and government alike is evidence of the challenge. News of cyberattacks, identify theft, and the hacking of corporate and government systems make users feel increasingly powerless to protect themselves or their data. When there is a data breach, the user often suffers most, though with little recourse.

With greater amounts of data being collected about many more aspects of our lives, we will have even more to lose in future data breaches. If the burden of risk is not more widely shared — through clearer legal accountability and greater investments in security — the decline in overall trust will accelerate.

> “
> A lack of trust on the Internet could lead to regression.
>
> Technologist, Africa

> “
> I think that trust has a very serious impact of future adoption and development of the Internet. With more data floating around, data protection and personal information security is another uncertainty that I can think of.
>
> Private Sector, Asia-Pacific

The lack of clear security *and* privacy standards for the Internet of Things raises the prospect of a “digital environmental disaster[3]” — a scenario in which abuse of connected objects by criminals, terrorists or even governments escalates to the point that the IoT environment becomes a polluted space in the eyes of consumers. A 2016 Accenture study of consumers in 28 countries concluded that “consumer technology industry does not have the fundamentals in place—and the consumer trust established—to push into more personalised and sensitive areas as it searches for the next wave of innovation”[4]. This same study noted that a lack of trust is already impacting the market for IoT as consumers remain cautious about whether or not the devices and their data will be secured.

Some, including Internet security expert Bruce Schneier, have gone so far as to suggest that, absent clear moral, ethical and political decisions, there might be a flight from connectivity as people reconsider how much should really be connected[5].

> “
> Security concerns may start to prevent users from going online, and once online may impact their usage, particularly with relation to sensitive political and personal issues”
>
> Civil Society, Europe

[3] https://otalliance.org/system/files/files/initiative/documents/iot_sharedrolesv1.pdf
[4] https://www.accenture.com/_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf#zoom=50
[5] http://www.elon.edu/e-web/imagining/surveys/2016_survey/internet_of_things_infrastructure.xhtml

Government actions also undermine user trust in the Internet around the world. Revelations about surveillance and emerging details about cyberattacks leave end-users wondering if they will be collateral damage in a conflict they are barely aware of and have little control over. Many politicians are framing security in ways that suggest a trade-off is needed between rights and freedoms on the one hand and security on the other. This caused one member of our community to suggest that "the Internet is not leading to a rights-based society but rather to a surveillance society".

> "Not meaning to sound gloomy, but all these shutdowns, filtering, and wide-scale surveillance have existing and potential users feeling like the Internet has become a massive platform for replicating offline oppression in the online world.
>
> Technologist, Caribbean

There is no single answer to the trust dilemma, but many current activities will help to improve the future Internet security environment for end-users. Stakeholders are devoting even greater resources to security, with one estimate suggesting global spending on cybersecurity may exceed $1 trillion between 2017 and 2021.[6] More messaging apps are using end-to-end encryption. Greater deployment has increased the volume of encrypted web traffic. IoT security frameworks are being developed. Internet companies are also taking steps to address concerns about fake news and violent online content. And, finally, serious global and regional efforts[7] to promote policy collaboration among stakeholders, including governments, are beginning to show results.

> "Is enough work being done on enhancing the web, making it more distributed, and more secure? Are we looking at new technologies for example how the bits we download each second can come from different sources to make it more difficult for people to know what you are doing online? I can imagine that this will happen one day soon and will have a great impact on the internet, and will make users more comfortable and trusting of the internet.
>
> Technologist, Middle East

Respondents already believe that the general public exhibits a degree of trust in the Internet today and predict that the general public will exhibit a higher degree of trust in the Internet (and low level of concern for most uses) in the future.[8]

Related to: Cyber Threats

[6] Cybersecurity Ventures' "Q2 2017 Cybersecurity Market Report": https://cybersecurityventures.com/cybersecurity-market-report
[7] For example: 2016 OECD Security Guidelines; 2017 African Union / Internet Society Internet Infrastructure Security Guidelines for Africa; Global Commission on Internet Governance; Global Commission on Cyber Stability.
[8] Future of the Internet Survey 2 - Question 32: "To what extent does the general public trust the Internet and its integration into daily life"?

AI and IoT will simultaneously empower and weaken users

Emerging technologies such as IoT and AI hold the potential to make the delivery of critical services more efficient and drive advancements in education, healthcare, agriculture and many other aspects of the economy and society. Armed with better information, citizens will be empowered to make more informed decisions and to hold governments and businesses accountable.

> “
> More sharing equals less privacy; people continue to trade convenience for security.
>
> Technologist, North America

As one technical expert in Europe suggested, “AI has the opportunity to increase transparency by making it easier to actually answer the question of where information is stored. So, in the future we can use our phone, our iPad, bracelet, computer, whatever kind of device we have, and ask where that specific company stores data about us and make the company accountable”. Individuals may be able to develop their own algorithms in order to track how they are being tracked. This scenario, one in which dramatic advances in Artificial Intelligence deliver results that have a positive impact on people’s lives, is only possible if humans remain in control of the technology and guide its development and deployment in ways that are consistent with human values.

There is another possible future in which AI and similar technologies are designed and deployed so fast, and with profound social impact, that the ethical and moral frameworks cannot keep up. In this scenario, advancements in AI and IoT may threaten human rights and personal freedoms and have huge implications for the transparency of decision-making and expectations of privacy. Algorithms use enormous quantities of information, much of it collected in ways that are not transparent to individuals. How will we ensure accountability when algorithms make decisions that affect people’s lives but are difficult to understand or to appeal?

> “
> Data collection is now a big privacy concern, especially when individuals are being observed by connected devices.
>
> Government, Africa

> “
> In the case of Big data and IoT who is responsible and accountable? We don’t know who to blame in case of abuse of a product or service: the designer, the manufacturer, the owner? How to include human right aspects into these artificial intelligent and IoT objects is a key question.
>
> Private Sector, Middle East

Personal Freedoms & Rights

Some users already worry about the vast amounts of their personal data being collected and feel powerless to protect their personal privacy. Already, systems use data profiling to draw inferences about individual beliefs, preferences or habits in ways that are deeply personal.

> People are worried — they don't know how much algorithms affect rights and data of persons.
>
> Civil Society, Middle East

With advances in AI, the collection of personal data will go beyond questions of privacy to a potential threat to personal autonomy. In a world where a lifetime of personal data-collection begins even before birth, and where that data is used to make decisions that deeply impact people's lives, people worry that they will lose the ability to question decisions and determine their own futures.

> The rise of data-driven services leads some to worry of a Minority Report-style future in which our course in life is mapped out for us, eroding our ability to make free choices. Then there's the worry that the data savvy might become a web-empowered elite, keen to keep those who are not digitally enabled firmly on the lower rungs of society.
>
> Private sector, Europe

Important work to ensure that human values drive technological and business advances is being done in the research, industry and policy communities. Whether the future Internet sustains our freedoms and rights, or whether it pushes them past the point of no return, will depend on whether this work can keep pace with the deployment of technology and has the continued buy-in and commitment of all stakeholders.

Related to: Artificial Intelligence; The Internet & the Physical World

Freedoms in light of the growing role of governments online

From its early days as an information-sharing network, the Internet empowered users and communities and enabled more transparent and accountable governance, raising awareness of human rights violations and gathering evidence for prosecution. Yet, as the scope and severity of cyber threats continues to grow, governments will put stronger systems in place, often in the name of national security, that will impact personal freedom and human rights. In some parts of the world, the Internet is being used as a tool for pervasive data collection, surveillance and control. This is reflected in an overall a deterioration in Internet freedom across the globe and we fear that, without a change of course, Personal Freedoms and Rights online may well be nearing a point of irreversible decline.

> “
> Liberal values are weakening around the world [which] doesn’t bode well for the Internet. Winter is coming.
>
> Civil society, North America.

Freedom House, a non-governmental organisation active in Internet policy, has documented a decline in Internet Freedom for the past six years[9]. Many of the Internet Society’s global community echo this sense of a decline in rights and freedoms — for them, restrictions such as Internet shutdowns are a consistent threat to their livelihoods, communities and future opportunities.

“keep it on” principles[10]

The very tools that facilitate human empowerment can also be used to constrain it, and as the Internet becomes part of everything we do, the temptation for governments to use it to constrain will only grow.

As many governments are pressured to respond to cyber threats, online hate and terrorism, even rights-respecting governments may see a false choice between security and human rights. For example, efforts to undermine encryption or ban anonymising tools like Tor for national security purposes threaten free expression and privacy of individuals everywhere. While new technologies can offer the promise of more efficiency and new services, they can also be used by governments — in the name of security –to create a surveillance society, undermining freedoms and privacy.

> “
> One of the biggest surprises is that democratic countries are seemingly starting to give up their leading role for an open Internet that supports online freedoms, in the wake of new national security threats and surveillance apparatus
>
> Civil Society, Europe

Although there is a collective responsibility to ensure that the Internet is not used as a tool of control, much of the burden will fall on the shoulders of the companies running networks or platforms and manufacturing connected devices. How industry and particularly the Internet companies react to government pressure will help determine the future of the Internet as a space for free expression or for censorship and surveillance.

[9] https://freedomhouse.org/report/freedom-net/freedom-net-2016
[10] https://www.internetsociety.org/african-youth-why-internet-matters

Personal Freedoms & Rights

> “It was thought that the Internet could bring democracy to all countries if they were connected to Internet but we learned that is not the case. The impact of Internet on politics is not as big as thought. Because of censorship there is a violation of human rights. China and Russia are protecting the stability of their countries. Western countries do not see it this way. This will be a big issue in the next 5–7 years.
>
> Government, Asia-Pacific

Stakeholders in our community still see the Internet’s underlying values of openness and global reach as fundamental and worth protecting. Indeed, it is clear that the core values of the Internet are not tied to any one geopolitical ideology — they are seen as universal.

> “The Internet will be increasingly used for education, to make economic transactions, to make political decisions and to defend our rights. Attacks on privacy will become more apparent. Citizens will be more aware of the risks and threats that exist on the Internet.
>
> Civil Society, Latin America & Caribbean

At the same, these values of openness and global reach will become more tenuous and cannot be taken for granted. All stakeholders will need to be vigilant and persistent if we are to maintain these core values in the face of the increasing claims of national security and public order. New and emerging technologies may well be part of the solution: rather than using them to undermine freedoms and rights we should use them to bolster the Internet’s core values of openness and global reach and counter the global trend of weakening freedoms and human rights.

Related to: The Role of Government; Cyber Threats