Geneva Internet Platform
DigitalWatch
NEWSLETTER

You receive hundreds of pieces of information on digital policy.
We receive them, too.
We decode, contextualise, and analyse them.
Then we summarise them for you.

DIGITAL POLICY TRENDS IN FEBRUARY

THE ICT INDUSTRY'S EVOLUTION IN DIPLOMATIC EFFORTS

Microsoft's proposal for a Digital Geneva Convention marks a new phase in the Internet industry's diplomatic efforts.

Microsoft is among the few Internet companies that have embraced diplomacy as an approach to shaping global public policies. For example, in 2015, after following closely the diplomatic dialogue shaping norms of state behaviour in cyberspace and confidence-building measures (CBMs), especially within the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) and the Organization for Security and Co-operation in Europe (OSCE), Microsoft proposed a set of cyber-norms for states, which was further updated with the proposal of cyber-norms for the ICT industry in 2016.

The industry's more active role in digital policy, including its role in solving the social costs of the fast digital developments, was predicted earlier this year. Taken forward, the implementation of the proposed convention would need to rely on co-operation and shared responsibility between governments and the Internet industry. *More on page 7.*

THE RISE OF FAKE NEWS

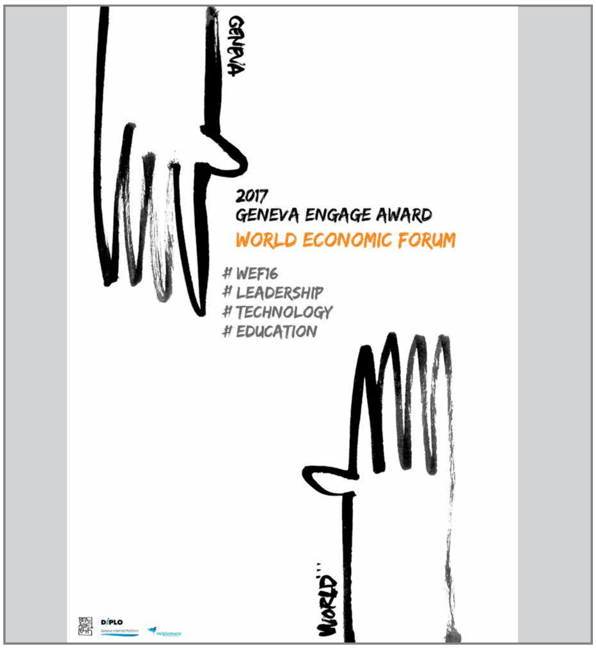
Fake news is a growing concern for governments, users, and the business sector. Fake news gives rise to a wide range of questions, from philosophical (truth in the modern era), to operational (attribution of fake news), to security questions (use of fake news for political aims).

Perhaps, the most immediately concerned stakeholders are Internet companies on whose platforms fake news is spreading. Tech companies, especially social media networks, suffered a backlash following the US Presidential campaign, and are still being widely criticised over the spread of fake news through their platforms, leading them to take several steps towards tackling the spread.

This development has given rise to several issues, a few of which are listed here. The first relates to terminology: *fake news* – information deliberately fabricated – is dominating the headlines. Yet, *false news* – incorrect information, which may or may not be deliberate – is also an issue. Using the terms interchangeably is common, misleading, and damaging for public debates.

Continued on page 3

The second Geneva Engage Awards honoured the most effective Geneva-based organisations in social media engagement in 2016. Among the award winners was the World Economic Forum. *More on page 2.*



IN THIS ISSUE

BAROMETER

The observatory looks at global developments in February. Cybersecurity, digital rights, and jurisdiction were particularly prominent.

More on pages 4 and 5

FAKE NEWS

FAKE

Discussions about fake news have continued to dominate the public debate. What are its implications and spillover effects, and what's behind the media frenzy?

More on page 6

GENEVA DIGITAL CONVENTION

Microsoft's call for a Digital Geneva Convention has attracted the attention of the digital policy community. What should it address, and how should it be implemented?

More on page 7

FEBRUARY IN IG HISTORY

Which developments took place in February, in the history of Internet governance (IG)? We take a look at the anecdotes.

More on page 8

Published on 28 February 2017, by the Geneva Internet Platform (GIP) and DiploFoundation | Contributors: Ana Andrijević, Stephanie Borg Psaila, Jovan Kurbalija, Roxana Radu, Vladimir Radunović, Barbara Rosen Jacobson, Sorina Teleanu | Design by Viktor Mijatović, Diplo's CreativeLab | The Brazilian version in Portuguese is available at dig.watch/newsletter | In addition to the *Geneva Digital Watch* newsletter, you can find in-depth coverage of developments on the *GIP Digital Watch* observatory (dig.watch) and join discussions on the last Tuesday of every month online, at local hubs, or at the Geneva Internet Platform (dig.watch/briefings) | Send your comments to digitalwatch@diplomacy.edu

GENEVA DIGITAL DEVELOPMENTS

ITU Council Working Group (CWG) Meetings

Several working groups of the International Telecommunication Union Council (ITU Council) held meetings in February. The meeting of the Child Online Protection CWG (2 February) reviewed initiatives, activities, and projects in the area of child safety online, such as the outcomes of an online consultation with youth on cyberbullying. The CWG on International Internet-Related Public Policy Issues held an open consultation (3 February) dedicated to discussions and the sharing of experiences and best practices on the topic of Developmental Aspects of the Internet. The importance of involving stakeholders from the private and the public sectors in efforts aimed at filling the gaps between countries and between men and women in the use of the Internet was repeatedly underlined during the debates. The open consultation was followed by the group's ninth meeting (6–7 February). The CWG on WSIS: Implementation of Outcomes (7–8 February) discussed aspects related to the ITU's role and activities in the World Summit on the Information Society (WSIS) facilitation, implementation, and follow-up, as well as ITU activities in relation to the 2030 Agenda for Sustainable Development.

Geneva Engage Awards 2017

The second annual Geneva Engage Awards, held on 8 February 2017, honoured the most effective Geneva-based organisations in social media engagement in 2016. The Awards, an initiative of DiploFoundation and the Geneva Internet Platform (GIP), supported by the Canton of Geneva and Twiplomacy, were awarded to three winners for their effective campaigns, interactive messages, and public engagement, in three categories: the World Health Organization, in the International Organisations category; the World Economic Forum, in the Non-Governmental Organisations and Non-Profits category; and the Permanent Mission of the USA to the United Nations in Geneva, in the Permanent Missions category. The panel discussion that followed focused on capacity building proposals for increasing the 'digital footprint' of permanent missions and organisations from small and developing countries.

WSIS Forum 2017 Open Consultation Process: Second Physical Meeting

The second physical meeting was held on 14 February at the ITU headquarters in Geneva. The meeting represented the third phase of the WSIS Forum Consultation Process, and was mainly dedicated to discussions on the thematic aspects of and innovation in the format. It was explained that the 2017 edition of the WSIS Forum will focus on the implementation of the sustainable development goals (SDGs) through the use of information and communication technologies (ICTs), under the overarching theme 'Information and Knowledge Societies for SDGs'. As presented by ITU representatives, the preparations for the Forum will be clustered around five types of activities: join, share, win, interact, and sponsor. With regard to the format of the Forum, it was noted that it will include WSIS Action Line facilitation meetings, WSIS Stocktaking and Prizes, partnerships on measuring ICTs for development, a regional commissioners' meeting, country workshops, and thematic workshops.

UN Group of Governmental Experts: Third Session

The third session of the UN GGE was held on 20–24 February in Geneva. The group continued work on the preparation of its final report, which is expected to be ready by the end of its fourth and last meeting, in June 2017. The UN GGE is expected to respond to some of the emerging concerns in the field of cybersecurity, including how to ensure the implementation of the existing voluntary and non-binding norms and CBMs; what should be the interplay between the UN GGE and regional organisations like the OSCE, the Association of Southeast Asian Nations (ASEAN) Regional Forum, and the Organization of American States (OAS), which also work on developing cybersecurity measures; and what should be the future of the GGE – should it continue for another round, be extended to include more states, or be replaced by a different body for a longer-term dialogue or by a standing committee for monitoring the implementation of the norms and CBMs.

Briefing for Heads of Missions: Digital Policy in South Eastern Europe

The briefing was held on 20 February 2017 at the Geneva Internet Platform, and was organised in partnership with the Permanent Mission of the Republic of Macedonia to the UN in Geneva. The event was held in preparation for the South Eastern European Dialogue on Internet Governance (SEEDIG), a sub-regional Internet Governance Forum (IGF) initiative recognised by the UN-led IGF, which will hold its third annual meeting on 24–25 May 2017 in Ohrid, Macedonia. The briefing focused, in particular, on cyber issues which are addressed in Geneva and are of relevance for the region, such as online human rights, cybersecurity, and digital trade. The GIP will provide permanent missions with regular updates on digital policy in the preparation for the IGF meeting, which will be held in December 2017 in Geneva.

Media Cybersecurity Seminar 2017

The seminar, organised by the European Broadcasting Union (EBU) on 21–22 February, was mainly dedicated to media companies hosted in Europe, and was aimed at providing them with guidance on how to mitigate the increasing number of online security threats. During the seminar, the EBU gave an overview of security standards and best practices for media companies. Other tutorials and presentations focused on issues such as content piracy and the evolution of threats and distribution methods, vulnerabilities in broadcast equipment, security in the Internet of Things (IoT), cybersecurity for journalists, security assessments for media companies, and the detection and mitigation of distributed denial of service (DDoS) and ransomware attacks.

DIGITAL POLICY TRENDS IN FEBRUARY

Continued from page 1

The second issue related to fake news concerns the extent of responsibility of intermediaries. While it is true that fake news is spreading mostly on their platforms, should they bear the brunt for all the content? Obliging them to sweep the platforms clean from fake news is tantamount to requiring them to become the *de facto* – or even *de iure* – content regulators.

The third relates to the sheer amount of content that Internet companies have to process. Can Internet companies be expected to plough through all the content, and does every platform have the capacity to do so? To what extent can artificial intelligence (AI) be used to filter news, and what about the risks of censorship?

Until governments and other stakeholders get to grips with these issues, companies are undertaking their own measures to root out fake news. We will continue to track the developments and any positions governments may take.

MINIMISING THE SOCIAL COSTS OF TECHNOLOGY

The impact of digital growth on jobs and social costs is one of the trends for 2017. It was an important theme in the US Presidential election; it will also remain high on the agenda of forthcoming elections in some European countries.

Benoit Hamon, the French Socialist Party's candidate for the upcoming presidential elections, is proposing the introduction of taxes for robots as a way to compensate human workers whose jobs become obsolete due to technological advancements. This came in the context of an ongoing debate on the introduction of a universal basic income – an idea that has already emerged in countries including Finland, India, and Scotland.

In explaining his proposal, Hamon noted: 'When a worker is replaced by a machine, the wealth created benefits the shareholders. I propose, therefore, to tax this wealth – by applying the social contributions on the whole of the added value and not just on the work.'

The French candidate's proposal, however, may not find favour in the EU, after the European Parliament voted against a universal basic income to compensate for disruptions brought by advancements of the digital industry.

Many of the controversial proposals in the initial report – elaborated by the Committee on Legal Affairs – were rejected by the Parliament. Among these, in fact, was the proposal to compensate individuals for disruptions brought on the labour market by robots and other AI systems.

The irony is – as Hamon pointed out – that while the industry is generating significant wealth through technological developments, sometimes to the detriment of workers whose livelihoods are disrupted, the contribution of the Internet industry in providing social stability and cohesion has been limited.

While the introduction of a universal basic income will continue to be debated, pressure on the industry is likely to increase with the fast developments in the fields of AI and robotisation.

THE USE OF SEARCH WARRANTS FOR DATA STORED OVERSEAS

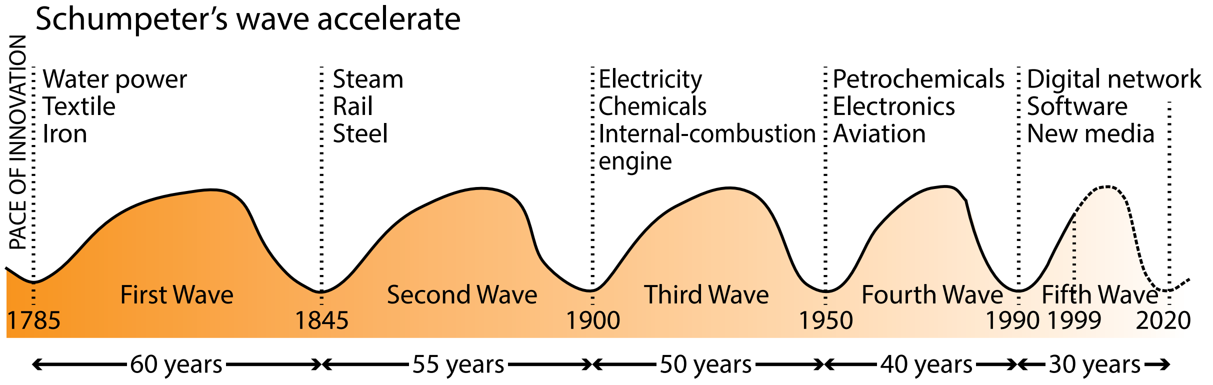
Juridical access to data hosted overseas by US Internet companies has come into focus with Microsoft's case last year when the Appeals Court declared that search warrants could not be used to disclose content held overseas.

A Philadelphia court, however, ruled that Google must comply with the FBI's search warrants and hand over data stored outside the USA. Unsurprisingly, Google has said it will appeal the ruling: 'The magistrate in this case departed from precedent in the case of Microsoft, and we plan to appeal the decision.'

Courts in the USA, Europe, and worldwide will continue to shape digital policy.

Turn to pages 4-5 for more digital policy developments in February.

The Schumpeterian Cycle of Innovation and Entrepreneurship



In the digital era, Schumpeter's creative destruction theory is often used to describe the disappearance of old industries and jobs and the appearance of new ones.

DIGITAL POLICY: DEVELOPMENTS IN FEBRUARY

Global IG architecture

increasing relevance

Microsoft has called for a Digital Geneva Convention, outlining six aims, and calling on both governments and the private sector to do more in the area of cybersecurity. In the same post announcing the proposal, the company's president also suggested that a safer cyberspace requires the collective action of the tech sector operating as a trusted and 'neutral Digital Switzerland'. In a similar, but unrelated post, an Indiana University professor asks whether cybersecurity should be a human right. Both posts emphasise the involvement of International and Digital Geneva as a centre for UN efforts to ensure global cybersecurity. *More on pages 1 and 7*

A new global multistakeholder body – the Global Commission on the Stability of Cyberspace – was launched during the Munich Security Conference. Headquartered in The Hague, the commission is tasked with developing proposals for norms and policy initiatives to improve the stability and security of cyberspace.

Sustainable development

increasing relevance

At the South Asian Speakers' Summit on Achieving the Sustainable Development Goals (18–20 February, Indore), speakers of parliaments from South Asian countries adopted the Indore Declaration, which calls for the 'sharing of knowledge, information, research support and capacity-building programmes for achieving the SDGs'.

Technology industry body techUK has called on G20 countries to prioritise innovation and digital technologies as key towards achieving the SDGs, and presented a series of recommendations aiming to 'advance privacy protections, enhance national security and data security, and enable the cross-border data flows'. GSMA and the UN Foundation launched the initiative Big Data for Social Good, during the Barcelona Mobile World Congress, to accelerate the mobile industry's input to achieving the SDGs.

Security

increasing relevance

The US delegate to the UN GGE has suggested that the group focuses on operationalising existing norms, i.e, on ensuring that already-defined norms are implemented. The UN GGE met for the third time on 20–24 February.

The second edition of the *Tallinn Manual* has been published. According to *Tallinn Manual 2.0*'s analysis, cyber events do not occur in a legal vacuum and states have both rights and obligations under international law.

E-commerce & Internet economy

same relevance

Uber has announced that it will suspend its services in Taiwan, following disputes with Taiwanese authorities. Uber had been operating in Taiwan as an Internet-based platform, and not as a provider of transportation services, which authorities ruled illegal.

A Brazilian labour court ruled that an Uber driver is an employee of the company and is entitled to workers' benefits. The judge also ordered Uber to pay one driver around $10,000 in compensation for overtime, night shifts, holidays, and expenses, such as gasoline and water. The company, expected to appeal, cited a contradictory ruling issued by another labour court in the same Brazilian state a few weeks before.

Malta has proposed that Europe should become the Bitcoin continent. 'The rise of crypto currencies can be slowed', the Prime Minister said during a Brussels event, 'but cannot be stopped.'

Digital rights

increasing relevance

The continuing government Internet ban in English-speaking areas of Cameroon is paralysing banks and affecting the economy. The ban was implemented in an attempt to quash opposition, but the lack of Internet has affected business and other areas. UN Special Rapporteur on freedom of expression, David Kaye, has urged the government to restore Internet services, to comply with international law and human rights.

Facebook and Google are co-operating with French news organisations to minimise the risk of fake news affecting France's upcoming presidential election. The collaboration plans to launch new fact-checking tools. Facebook is taking similar steps in Germany, while Google has also introduced the fact-checking tool for users in Argentina, Brazil, and Mexico. In Venezuela, CNN in Spanish was blocked after it was accused as spreading fake news. *More on pages 1 and 6*

Ireland's Data Protection Commissioner is challenging Facebook's model contracts, a legal arrangement under which the data of EU citizens is transferred across the Atlantic.

Comments made by the Secretary of the US Department of Homeland Security suggested that the Department could require non-US travellers on their way to the USA to disclose passwords to their social media accounts as a condition of entering the country. A coalition of human rights and civil liberties organisations, trade associations, and experts issued a joint statement expressing concern.

Jurisdiction & legal issues

increasing relevance

A Philadelphia judge has ruled that Google must comply with FBI search warrants, for Gmail messages stored outside the USA, as a part of a domestic fraud investigation. Google will appeal.

The European Parliament has reached an agreement which will soon allow Europeans to fully use their online subscriptions to digital content when travelling within the EU. The agreement is related to the EU's plan to modernise its copyright rules, which was proposed in the European Commission's Digital Single Market strategy.

The Swedish Court of Patent and Market Appeals ordered an Internet service provider (ISP) to block access to The Pirate Bay and Swedish streaming portal Swefilmer, following EU laws and similar judgments in Australia, Belgium, Finland, and France. Swedish ISPs have expressed concern, as their obligation to monitor and evaluate digital content could constitute 'a dangerous path to go down'. In the UK, Google and Microsoft reached an agreement with the UK government and the creative industry to limit pirated films and music online.

Infrastructure

increasing relevance

ICANN proceeded with the delegation of the .africa top-level domain (gTLD), after a decision by a California Superior Court. The court denied DotConnectAfrica's (DCA's) second motion for a preliminary injunction to stop the delegation of .africa to ZA Central Registry.

The race to deploy 5G in the market has sped up. The ITU has agreed the minimum network requirements of 5G networks. The proposed framing standard is to be approved by the ITU-R Study Group 5 in November 2017 and should serve as a basis for further standardisation of the International Mobile Technology 2020 environment (IMT-2020) and its 5G networks. Meanwhile, Verizon announced a commercial pilot 5G deployment in 11 markets across the United States by mid-2017.

An overview of the status of Internet Protocol (IP) address space in 2016, published by APNIC's Chief Scientist, shows that the number of individual allocations of IPv6 addresses rose by some 20% in 2016 compared to 2015. The countries that received the largest number of IPv6 allocations in 2016 were Brazil, the USA, China, Germany, Australia, the UK, the Netherlands, Russia, India, and Indonesia.

Cisco's *2017 Annual Cybersecurity Report* suggests that spam accounted for 65% of the total e-mail volume in 2016. The volume of spam last year is close to the record levels seen in 2010. This is due to an increasing number of spam-sending botnets, 8–10% of which are malicious.

Net neutrality

same relevance

The US Federal Communications Commission (FCC) has set aside its January 2017 report on zero-rating practices. The report had concluded that zero-rating services offered by AT&T and Verizon presented risks to consumers and competition. A few days after the rescission, Democratic members of the US Senate expressed their support for strong net neutrality rules, and said that they would not allow action by the FCC or Congress that undermine those rules.

Chinese company Alibaba is considering providing free Internet in India and is currently in negotiations with telecom operators and WiFi providers in the country. It remains to be seen what kind of Internet services the company will provide and whether there will be any implications for the principle of net neutrality, for which India has been strongly advocating.

New technologies (IoT, AI, etc.)

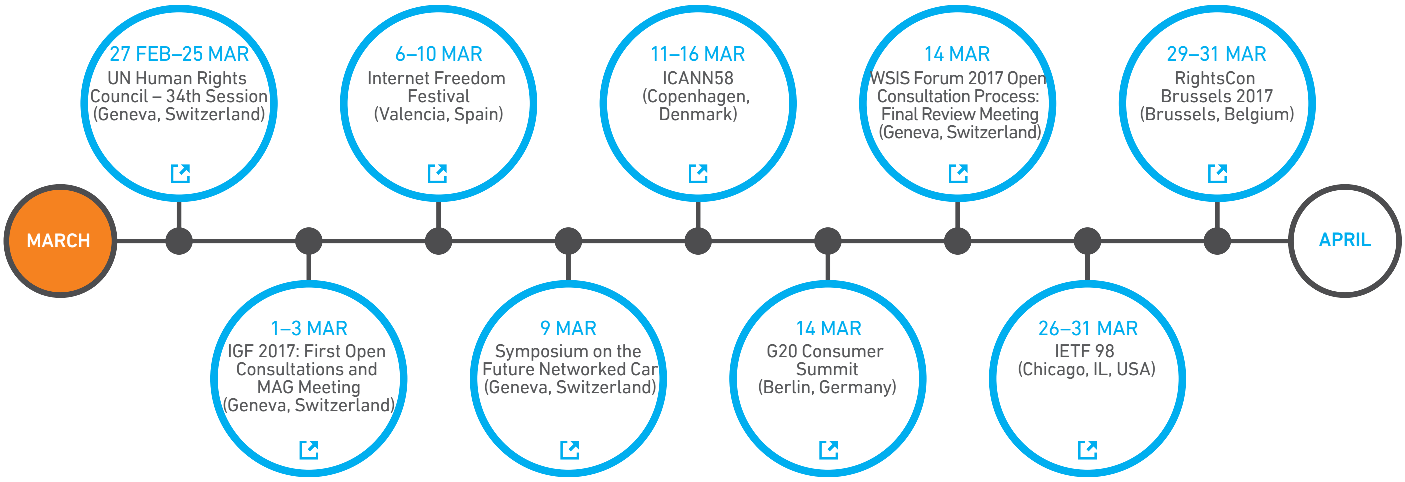
same relevance

AT&T, IBM, Nokia, Palo Alto Networks, Symantec, and Trustsonic have formed the IoT Cybersecurity Alliance, aiming to 'help customers address IoT cybersecurity challenges, demystify IoT security, and share best practices'. A report on *The Internet of Evil Things* shows that connected devices will be a major security issue in 2017. On the other hand, IBM's Resilient Chief Technology Officer called for the creation of a new government agency to focus on regulating the IoT, especially from a security point of view.

According to the GSMA and Machina Research, Low Power Wide Area (LPWA) connections are set to exceed 2G, 3G, and 4G and become the leading technology for the IoT, with 1.4 billion connections by 2022. 'LPWA networks are an emerging, high-growth area of the IoT, designed to support machine-to-machine applications that have low data rates, require long battery lives, and operate unattended for long periods of time, often in remote locations.'

The application of drones for different services continues to grow, as Dubai plans to introduce flying drone taxi services next July. The passenger service will make use of autonomous electric drones that can carry one passenger for a distance of 31 miles, and will be remotely monitored and piloted from a centralised command centre.

AHEAD IN MARCH



MARCH

27 FEB–25 MAR
UN Human Rights Council – 34th Session
(Geneva, Switzerland)

1–3 MAR
IGF 2017: First Open Consultations and MAG Meeting
(Geneva, Switzerland)

6–10 MAR
Internet Freedom Festival
(Valencia, Spain)

9 MAR
Symposium on the Future Networked Car
(Geneva, Switzerland)

11–16 MAR
ICANN58
(Copenhagen, Denmark)

14 MAR
G20 Consumer Summit
(Berlin, Germany)

14 MAR
WSIS Forum 2017 Open Consultation Process: Final Review Meeting
(Geneva, Switzerland)

26–31 MAR
IETF 98
(Chicago, IL, USA)

29–31 MAR
RightsCon Brussels 2017
(Brussels, Belgium)

APRIL

For more information on upcoming events, visit dig.watch/events

FAKE NEWS: WHAT'S BEHIND THE MEDIA FRENZY

Discussions about fake news, ignited right after the US Presidential election in November 2016, have continued to dominate the public debate, as Internet companies increasingly face backlash over the spread of fake news on their platforms. Fake news has become a concern across time, regions, and the political spectrum, leaving many to wonder about its implications, spillover effects, and the role of 'truth' in today's Internet era.

A new post-truth era or an age-old phenomenon?

Connected to the hype around fake news, some have suggested that we are living in a post-truth era. Historians are debating whether fake news is something inherently new about today's society, or whether it is a continuation of the past. Many claim that fake news has always existed, pointing at antiquity, interwar Germany and Britain, and twentieth-century ideological struggles.

What digital media has introduced is the facility to disseminate news, which is arguably easier in an online environment that is loosely regulated, providing a more fertile breeding ground for fake news than ever before.

Fake news discussions beyond US shores

Most discussions about fake news have predominantly focused on its role in US politics. Yet, although the initial uproar about fake news might have been generated by the US elections, other countries are increasingly having to deal with their own fake news incidents.

In Europe, concerns have arisen over the fake media's potential to impact this year's elections in France, Germany, and the Netherlands. In the UK, the parliament is planning to launch an inquiry into fake news and the role of social media platforms, which are seen to 'have a responsibility to ensure their platforms are not being used to spread malicious content'.

Fake news has also entered the news ecosystems of a number of African countries, including Eritrea, Kenya, Nigeria, South Africa, and Zimbabwe, leading Nigerian Minister of Information and Culture, Alhaji Lai Mohammed, to claim that fake information 'poses a greater threat than insurgency and militancy'. Similar fake news incidents have been reported in Iran and India. In Latin America, the Venezuelan government blocked CNN in Spanish, accusing it of spreading fake news.

Dealing with fake news

The natural first responders – and most criticised actors – are the platforms on which fake news is published or can spread. Filtering and suppressing content that could possibly contain fake information risks infringing freedom of expression and might lead to a situation in which intermediaries are the arbiters of truth – a role that Facebook's CEO Mark Zuckerberg is 'extremely cautious' about. At the same time, fake news can lead to massive misinformation and adverse political consequences.

This delicate balance was also highlighted by Apple's CEO Tim Cook, who explained that the tech sector should not be stepping on freedom of speech and freedom of the press, but 'we must also help the reader'.

Dealing with fake news begs another question: Is it realistic for Internet platforms to be able to filter through the millions of posts that are published on their platforms every day? Can artificial intelligence provide solutions for automatic filtering, as it has been suggested by the Internet industry?

Flagging and fact-checking

Facebook's and Google's current approach is to flag fake news and to remove posts that are violating their terms of use or local regulations. In the midst of the US elections, Google introduced its Fact Check tag in October 2016, which has now been launched in Argentina, Brazil, France, Germany, and Mexico. The companies are also co-operating with French news organisations to introduce new fact-checking tools, while Facebook's fake news filtering tools are being tested in Germany.

Several fact-checking initiatives have also been launched outside the realm of Internet companies. The EU established the East Stratcom Task Force to address 'Russia's ongoing disinformation campaigns', and has discredited 2500 stories since its creation in June 2015.

Similar initiatives have been implemented in Finland and the Czech Republic. Africa Check promotes accurate information in Africa's public debates and media outlets.

The German government has taken concrete steps against fake news with an action plan that would make it easier to filter fake information from the Internet, protect victims of fake news, and fine Internet platforms that do not comply with the plan with a suggested figure of €500,000.

Nevertheless, questions remain whether such initiatives will have a meaningful effect when they are faced with the enormous amount of potentially falsified content that is being shared on social media platforms worldwide.

Awareness-raising and immunisation

The key may be in awareness-raising and education. Apple CEO Tim Cook echoed an increasingly heard message, calling for 'massive information campaigns' targeting every demographic. South Africa's Eyewitness News website implemented a fake news guide last month, alerting all visitors to its websites 'Don't fall victim to fake news!' and in the USA, schools have tentatively started to adapt their curriculum towards better awareness of fake news and fact-checking.

Cambridge University's innovative solution is to provide a fake news 'vaccine'. Researchers propose 'pre-emptively exposing' readers to small bits of fake information, 'to provide a cognitive repertoire that helps build up resistance to misinformation, so the next time people come across it they are less susceptible'.

Follow the latest developments on how stakeholders are tackling the issue of fake news, and how fake news is impacting digital policy, on our dedicated page on the GIP Digital Watch observatory.

DIGITAL GENEVA CONVENTION: PROTECTING CIVILIANS FROM CYBERATTACKS

Microsoft's recent call for a Digital Geneva Convention – which should 'commit governments to avoiding cyber-attacks that target the private sector or critical infrastructure or the use of hacking to steal intellectual property' – attracted the attention of the digital policy community. It brought into focus the idea that, in the search for a more secure and stable Internet, Internet companies need to engage with governments and work together on reasonable policy arrangements. The proposal gave rise to many pertinent questions related to the future of digital governance, in particular in the security field. Here, we address some of them.

What is the main aim of a Geneva Digital Convention?

The Geneva Digital Convention, proposed recently by Brad Smith, Microsoft's President and Chief Legal Officer, should create binding rules out of the voluntary norms on secure cyberspace developed by the UN GGE and regional organisations. Embedded within a convention, these and few other additional norms could become a legal obligation, with the corresponding enforcement mechanisms. According to Microsoft's proposal, the convention should motivate states to adhere to the agreed norms.

What should a Geneva Digital Convention regulate?

The six principles proposed by Microsoft are typically based in national security, related to both defensive and offensive cyber-operations. They are a mix of policy and legal regimes. Principle 1 could be classified as the *ius ad bellum* principle, dealing with justification and prevention of conflicts; principles 3, 4, and 5 have a strong cyber-disarmament focus; principles 2 and 6 are applicable both in conflict and peace-time operations.

Moving from the six principles, Microsoft's arguments shift towards **protecting citizens** in the case of conflict – which in legal terms is known as *ius in bello* – or even broadly speaking towards what we might call human cybersecurity.

Human security is anchored in the protection of human wellbeing. Since human wellbeing increasingly depends on digital space, the question of human cybersecurity is likely to come more into focus.

If Microsoft's proposal aims to focus on **human cybersecurity**, this will bring developmental aspects into discussion – ensuring means for people to achieve cyber wellbeing (access to the Internet, development of local content, etc.), as well as human rights issues, including a potential right to safe access to the Internet.

How could the proposed convention be implemented?

Smith introduced ideas aiming to serve as a potential inspiration for a multistakeholder implementation of the Convention. While governments should ensure rule-based digital governance, shared responsibility should involve the private sector that runs most of the Internet, and the technical community that sets most of the technical standards.

An independent organisation should be a public-private partnership that can deal with attribution – the main challenge in addressing cyber-attacks. Potential inspiration can be found in the Montreux process for private military and security companies.

Smith mentions the role of the International Atomic Energy Agency (IAEA) in nuclear non-proliferation as a possible inspiration for the future cybersecurity organisation.

The Red Cross is also suggested as a potential model for future cyber arrangement. The main analogy is to the International Committee of the Red Cross (ICRC), the pillar organisation of the Red Cross movement and implementer of the Geneva Conventions. Other parts of the Red Cross movement could also provide some inspiration, such as national organisations that have an auxiliary role to governments. The role of Computer Emergency Response Teams (CERTs) could be upgraded in this direction. They may not be part of government but their role could be recognised as a public role in protecting civilians and entities in the event of a cyber-attack.

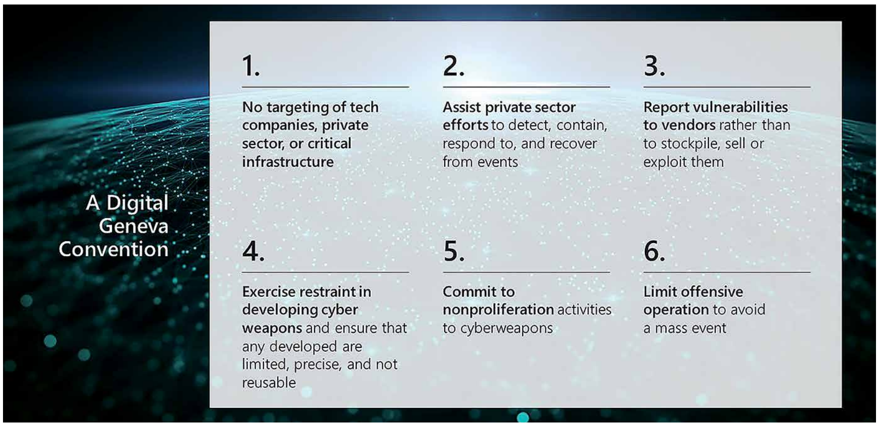
How can neutrality be achieved in cyber arrangements?

Neutrality is frequently mentioned in the Microsoft proposal. Neutrality (or the lack of it) could make or break any future cyber arrangement. Microsoft links the proposal to Geneva (Geneva Digital Convention) and Swiss neutrality ('neutral Digital Switzerland'). As Geneva and Switzerland are sought for the establishment of good offices and as mediators in times of traditional conflict, they may extend this role to cyber conflict and crisis. The centrality of Geneva – as an important hub for digital policy, among other policy areas – also comes into focus in the Microsoft proposal.

What are the next steps?

The future cyber governance architecture will be discussed in many contexts during 2017, including within the UN GGE, and at the 12th IGF meeting.

Microsoft's proposal for the Geneva Digital Convention provides inspiring analogies, asks many questions, and initiates discussion on the future of digital governance, in particular in the security field. While there are major differences among stakeholders, there is also considerable convergence and many common interests. These common interests provide some optimism for future discussions on and negotiations of digital governance.



A Digital Geneva Convention

1. **No targeting of tech companies, private sector, or critical infrastructure**

2. **Assist private sector efforts** to detect, contain, respond to, and recover from events

3. **Report vulnerabilities to vendors** rather than to stockpile, sell or exploit them

4. **Exercise restraint in developing cyber weapons** and ensure that any developed are limited, precise, and not reusable

5. **Commit to nonproliferation** activities to cyberweapons

6. **Limit offensive operation** to avoid a mass event

Credit: Microsoft

This article is based on an analysis of the proposal by Dr Jovan Kurbalija, director of DiploFoundation, and head of the Geneva Internet Platform.

FEBRUARY IN INTERNET GOVERNANCE HISTORY

From the development of advanced computing systems and the introduction of Internet standards and protocols, to the launch of today's widely used online services and the elaboration of policies shaping the use and evolution of digital tools, the historical timeline of the Internet and Internet governance is as interesting as it is remarkable. Here, we take a look at main developments that took place in February.

Visit the *GIP Digital Watch* observatory and follow us on Twitter and Facebook for more anecdotes.

14 February 1946
The Electronic Numerical Integrator and Computer (ENIAC) – sometimes described as the first fully electronic computer – was announced to the public, at the University of Pennsylvania.

19 February 1971
The first warrant to search a computer storage device was issued, in the USA.

28 February 1990
The Advanced Research Projects Agency Network (ARPANET) was officially decommissioned, after 30 years of service. It was the first network to implement the Transmission Control Protocol/Internet Protocol (TCP/IP) suite.

8 February 1996
John Perry Barlow posted 'A Declaration of the Independence in Cyberspace', containing the often quoted call: '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.'

22 February 1999
The first full-service bank accessible only via the Internet – First Internet Bank, Indiana, USA – opened to the public.

4 February 2004
Mark Zuckerberg launched Thefacebook, which later became the popular social network, Facebook.

10 February 2004
Flickr, the photo sharing website, was released at the O'Reily Emerging Technology Conference.

8 February 2005
Google Maps was launched to the public.

15 February 2005
The YouTube.com domain name was activated.

3 February 2011
The Number Resource Organization announced that the free pool of available Internet Protocol version 4 (IPv6) resources was fully depleted.

Subscribe to *GIP Digital Watch* updates at www.giplatform.org/digitalwatch