DIGITAL POLICY TRENDS IN MARCH

1. CHINA OUTLINES NEW CYBER DIPLOMACY

Early this month, China launched its International Strategy of Cooperation on Cyberspace which sets out the country’s policy and position on cyber-related international affairs. China’s cyber diplomacy rests on cyber sovereignty in the political realm and digital global integration in the economic realm.

The Chinese strategy reiterates China’s well-known position in the digital field: it supports a multilateral approach, yet it opens possibilities for other stakeholders to play their respective roles via a ‘multi-party’ approach. The strategy does not refer to the term ‘multistakeholder’.

It also supports the formulation of norms of state behaviour (within the UN framework), making reference to the work of the UN Group of Governmental Experts, and the Shanghai Cooperation Organization’s International Code of Conduct for Information Security.

China is recommending that basic Internet resources be equitably distributed, and that critical infrastructure be managed jointly. Reference is made to the management of root servers, indicating that the Internet Corporation for Assigned Names and Numbers (ICANN) still needs to become a truly independent international institution. The country will work to ensure not only the Internet’s security, but also its stability.

With regards to the Internet Governance Forum (IGF), China proposes institutional reform, including strengthening its decision-making capacity, and introducing transparent procedures in its ‘member election’.

The strategy prominently features equality in co-operation on a wide range of issues, from the management of critical information infrastructure, to the sharing of benefits of the information society, and the development of norms.

2. WIKILEAKS REVEALS THE US CENTRAL INTELLIGENCE AGENCY’S HACKING ARSENAL

WikiLeaks latest disclosure, dubbed Vault 7, involves over 8000 pages of confidential documents of the US government dating from 2013 to 2016. The documents describe the CIA’s ability to hack phones, computers, and smart devices.

The leaks come a year after the Apple/FBI case in which Apple was ordered to assist the FBI with unlocking data from a terrorist’s cell phone. The lawsuit was dropped after the FBI obtained the ‘assistance of a third party’.

UBER: RAPID EXPANSION, RISE IN LEGAL CASES

The development of new business models such as the sharing economy has been accompanied by a rising number of legal and regulatory issues. We explore the main issues, and look into the court cases and rulings involving Uber. More on page 7.

The observatory looks at global developments in March. Cybersecurity, digital rights, and net neutrality were among the most prominent issues.

A new resolution adopted by the Human Rights Council, and a second report by the UN Special Rapporteur on privacy brought digital rights under focus.

How is data shaping our future? How does data intersect with digital policy? How are Geneva-based organisations using data? Discover our latest initiative...
The 34th session of the UN Human Rights Council (HRC), took place from 27 February to 24 March and featured high-level discussions on various human rights-related issues, including the right to privacy, rights of persons with disabilities, and rights of the child. During the session, the UN Special Rapporteur on the right to privacy presented his report, which focuses on governmental surveillance activities from a national and international perspective, and recommends, among others, that states consider the adoption of a legal instrument to regulate surveillance in cyberspace. The HRC also adopted a Resolution on the right to privacy in the digital age which reaffirms the principle that the same rights that people have online must also be protected online, and calls on states to take measures aimed at guaranteeing and protecting the right to privacy, including in the context of digital communications.

The meeting, on 1-3 March, brought together members of the Multistakeholder Advisory Group (MAG) and the broader IGF community for discussions on the IGF 2016 meeting and intersessional processes, as well as the programme and structure of the IGF 2017 meeting and other IGF activities. The Open Consultations focused on issues such as maximising the opportunities of having the IGF 2017 meeting hosted in Geneva, the home of many international organisations; the possible development of a long-term strategic plan for the IGF; and ways in which the IGF could increase its visibility, including working on Internet governance issues. During the MAG meeting, members discussed the IGF workshop review and evaluation process, and agreed on an overarching theme for IGF 2017 – “Shape your digital future.” A decision was also made to continue the IGF intersessional work on “Policy options for connecting and enabling the next billion(s),” as well as the Best Practice Forums on gender and on cybersecurity.

The symposium, on 9 March, jointly organised by the International Telecommunication Union (ITU) and the United Nations Economic Commission for Europe (UNECE), aimed at providing a platform for discussion among different stakeholders – vehicle manufacturers, governments, and information and communications technology industries – on the future of vehicle communication and automated driving. The event comprised five thematic panels, featuring debates on the advantages and challenges of automated driving, the benefits of fifth-generation mobile networks or wireless systems for the development of automated driving, potential changes brought about by artificial intelligence (AI) to current transport systems, the relationship between connected vehicles and automated driving, and cybersecurity threats to automotive systems.

The final review meeting, on 14 March, was dedicated to discussions on the thematic aspects and innovations on the format of the World Summit on the Information Society (WSIS) Forum 2017, scheduled for 12-16 June. An overview was given of the preliminary results of the online and physical consultations, held between September 2016 and March 2017. It was explained that the submissions received from civil society organisations, international organisations, governments, academia, and the private sector will feed into the Forum’s agenda and programme. Discussions then continued on aspects related to session formats for the various segments of the Forum’s programme (policy statements from ministers and other high-level representatives, a ministerial roundtable, plenaries, workshops, open debates, lightning talks, etc.), possible themes and titles, and strengthening the Forum outcomes.

The European Broadcasting Union (EBU) conference, on 21–22 March, brought together heads of digital, marketing, communications, and legal departments within public service media organisations, as well as technologists and academics, to share best practices for big data media strategies. The first day focused mainly on how to build trust and obtain social acceptance of big data, by taking into consideration ethics laws and human rights. There were also discussions on the role of algorithms and platforms in facilitating users’ access to media content, and the utility of big data for journalism and reporting. The second day focused mainly on aspects related to the personalisation of media content according to audience’s preferences, with the ultimate goal of providing customers with personalised services and thus better experiences.

The workshop organised on 21 March by the ITU, aimed, among others, at promoting a better understanding of blockchain technologies and applications, and their various implications, including with relation to security and privacy. Following an introductory session on blockchain, discussions revolved around security and trust mechanisms for blockchain technologies; policy and regulatory implications of blockchain; the use of blockchain technologies to improve cybersecurity, privacy, and online trust; and standardisation efforts on blockchain in international standards bodies. There were also discussions on potential issues that the ITU Telecommunication Standardization Sector (ITU-T) Study Group 17 on Security could analyse and review with regard to blockchain standardisation, as well as possible ways forward in terms of collaboration with other stakeholders.

**Geneva Digital Developments**

**UN Human Rights Council – 34th Session**

**IGF 2017: First Open Consultations and MAG Meeting**

**Symposium on the Future Networked Car**

**WSIS Forum 2017 Open Consultation Process: Final Review Meeting**

**EBU Big Data Conference**

**ITU Workshop on Security Aspects of Blockchain**

---

This icon indicates that there is more background material in the digital version. Alternatively, visit [dig.watch](http://dig.watch) for more in-depth information.
Vault 7 documents, however, reveal that the CIA was able to compromise the software of all the major vendors, including Apple, Microsoft, and Android, as well as those of producers of Internet of Things (IoT) devices such as Samsung, confirming that the agency was tracking vulnerabilities rather than reporting them to the vendors to patch them. The CIA was also able to trick major anti-virus programs, such as Kaspersky, BitDefender, AVG, and F-Secure software, to avoid detection of the intrusion into systems.

While some say this is merely old news, the leaked documents bring the interplay between privacy and security to the forefront yet again. Can citizens’ safety be ensured without compromising their right to privacy, or is the dichotomy between privacy and security true? At which point are authorities considered to have crossed the line? And more importantly, how should other stakeholders tackle cases of unlawful surveillance, proof of which continues to emerge regularly?

3. SURVEILLANCE TREATY PROPOSED BY THE UN SPECIAL RAPPORTEUR ON PRIVACY

After Microsoft’s proposal for a Digital Geneva Convention, the UN Special Rapporteur on privacy proposed a surveillance treaty. While proposals for a Digital Geneva Convention are aimed at preventing cyber-attacks that target the private sector or critical infrastructure, a surveillance treaty would co-exist alongside other instruments – such as the Cybercrime Convention – and be deemed to complement them.

A surveillance convention should address surveillance activities for national security purposes that fall beyond the scope of existing international instruments. The lack of regulation of this type of surveillance poses high risks for privacy protection.

4. EU BODIES DEMAND CHANGES IN SOCIAL MEDIA COMPANIES’ TERMS

Authorities in the EU are putting pressure on social media companies to change, within one month, their jurisdiction clauses and other terms of use which create an imbalance in the users’ rights and obligations.

The required amendments will address a number of issues identified by EU consumer protection authorities late last year, including: jurisdiction (social media networks cannot deprive consumers of their right to go to court in their member state of residence); misleading content (companies must remove any fraud and scams appearing on their websites that could mislead consumers, once they become aware of such practices); and termination of contracts (termination should be governed by clear rules and not decided unilaterally without a reason).

In the past few years, several courts – mostly in Europe – ruled that users could bring cases before courts in their country of residence. The amendments suggested by the EU authorities would further solidify this jurisdiction tenet, which – as the EU consumer bodies explained in their common position – finds legal basis in the EU’s Unfair Contract Terms Directive and the Regulation on the law applicable to contractual obligations (the so-called Rome I).

EU bodies have warned they would take enforcement action, if necessary, in the case of non-compliance.

5. ICANN’S 58TH MEETING REFOCUSES ON POLICY DEVELOPMENT

Unlike previous meetings which focused on the Internet Assigned Numbers Authority (IANA) stewardship transition and the strengthening of ICANN’s accountability, ICANN’s 58th meeting – held in Copenhagen, Denmark, on 11-16 March – refocused on policy development processes.

Discussions included the advancements on policies related to the new generic top-level domains (gTLD) and how to improve the next round(s) of new gTLD applications, mechanisms for disbursing the resources accrued from the gTLD auctions of the first round, and issues related to ICANN’s WHOIS policy, which will undergo comprehensive reform.

Data – an important tool for evidence-based policy development – was discussed in the context of transforming ICANN into a data-driven organisation. This follows the recent trend by organisations worldwide to use data generated from their activities to shed light on market-related practices and to inform policy processes. Learn more about the Geneva Internet Platform’s project on data-driven organisations.

The Digital Watch observatory’s team followed the discussions closely; thematic reports are available on the dedicated page. Discussions on ICANN’s policy development processes are expected to intensify at the next meeting in June, in Johannesburg.
These amendments to the Excise Tax Act will redefine ride-sharing firms, such as Uber, as taxi companies. This would end the tax advantages that they have over traditional taxi companies, forcing them to collect the goods and services tax for every ride.

The US Congress voted to repeal rules prohibiting Internet Service Providers from selling user data, in order to protect the right to privacy. The move is part of a broader effort to ensure legal certainty and position on cyber-related international affairs.

Preparations for IGF 2017 continued with the first round of Open Consultations and MAG meeting. The deadline for proposals is 3 May 2017.

At its 2017 Spring Meeting, the Broadband Commission for Sustainable Development committed to concrete actions that will stimulate the deployment of broadband infrastructures around the world. Members outlined the need for a new agreement between all broadband stakeholders with a view to achieve global connectivity and digital transformation.

A new report by the Commission’s Working Group on the Digital Gender Divide analyses and addresses the difficulties faced by women in realising the full potential of Internet access. The report notes that the gender gap widened from 2013 to 2016.

WikiLeaks released over 8000 pages of confidential documents of the US government, dating from 2013 to 2016, which provide detailed descriptions of the CIA’s ability to hack phones, computers, and smart devices. The leaks, dubbed Vault 7, reveal that the CIA was able to compromise software and IoT devices developed by major vendors including Apple, Microsoft, Android, and Samsung.

The US Department of Justice has indicted four Russians, including two officers of the Russian Federal Security Service, in relation to the 2014 Yahoo! e-mail breach. Over 500 e-mail accounts were compromised during the attack. One of the two indicted officers was charged with treason and arrested by Russian authorities last winter.

The Ministry of Defense of Singapore reported a cyberattack that compromised the personal data of 850 employees of the public service. Its internal network, containing sensitive data, was not breached, however. The French government has decided to abandon plans to allow its expats to vote online during the upcoming national elections, over fears of cyberattacks.

The Canadian government plans to amend its Excise Tax Act to redefine ride-sharing firms, such as Uber, as taxi companies. This would end the tax advantages that they have over traditional taxi companies, forcing them to collect the goods and services tax for every ride.

Russia’s Internet regulator Roskomnadzor has confirmed that LinkedIn will remain blocked until it agrees to move Russian user data to Russian territory. The network has been blocked since November.

In a report presented to the UN Human Rights Council during its 34th session, the UN Special Rapporteur on the right to privacy has suggested a legal instrument to regulate surveillance in cyberspace. The UN HRC adopted a resolution on the right to privacy in the digital age, in which the Council called upon states to respect and protect the right to privacy, including in the context of digital communications, and to take measures to put an end to violations.

RightsCon 2017, held in Brussels on 29-31 March, tackled challenges for digital rights from different angles, including data localisation, geo-blocking, and surveillance. The Court of Justice of the European Union has ruled that the right to be forgotten does not extend to company registers, which need to be public to ensure legal certainty.

The US Congress voted to repeal rules prohibiting Internet Service Providers from selling user data, including browsing history, without their consent. In the UK, Home Secretary Amber Rudd has called for Internet companies to co-operate with the government in the fight against terrorism, by providing police and intelligence agencies access to encrypted messaging services like WhatsApp. Internet blockage in Anglophone Cameroon reached past its 90th day, causing more damage to the country’s economy.

Social media companies have one month to make changes to their general terms of use to comply with EU consumer protection legislation, the European Commission has announced. These amendments will address a number of issues, including jurisdiction, misleading content, and termination of contracts.

The German government has published a draft law that will impose fines of up to €50 million on social networks that do not remove hate speech and fake news. Content that is considered ‘blatantly illegal’ needs to be removed within 24 hours, whereas other ‘law-breaking content’ should be taken down or blocked within a week. According to German Federal Minister for Justice and Consumer Protection, ‘Facebook and Twitter missed the chance to improve their takedown practices.’ Meanwhile, Google has apologised over advertisements appearing on extremist content after a large number of companies accused the Internet giant of ‘profiting from hatred’ and pulled their Google advertisements.

WIPO has reported a 10% increase in domain name cybersquatting cases in 2016. The generic top-level domains (gTLDs) with the most disputed domain names were .xyz, .top, and .club.
In the second public meeting since the IANA stewardship transition, discussions at ICANN58 re-focused on ICANN’s policy development processes, including those related to the New gTLD Program.\[ Read the GIP’s reports from ICANN58.\] Governments expressed dissatisfaction with the ICANN Board’s decision to allow the registration of two-letter domain names – including country codes – in new gTLDs, over fears that this would create confusion.\[ The Board has been advised to find a solution to meet these concerns.\] Meanwhile, registries of new gTLDs have asked ICANN for a temporary offset of registry fixed fees, given that a number of gTLD operators are struggling.\[ Starting in June, US telecom company Verizon will stop issuing new public static IPv4 addresses, due to a shortage in available addresses.\] ICANN has launched a testing platform in preparation for the root zone DNSSEC key signing key rollover, scheduled for 11 October 2017. DNSSEC is the protocol upgrade that ‘digitally signs’ domain names to prevent their misuse.

Security experts are expecting an increase in cyberattacks on the industrial IoT in 2017. The study by Tripwire Inc, which looked at industrial IoT deployment in organisations, revealed that 51% of the surveyed security professionals do not feel prepared for security attacks.\[ But the US Federal Trade Commission (FTC) is cautious about regulating the sector. If there is potential harm to consumers, the FTC believes it should not act until that harm manifests.\]

Researchers at the University of Rochester have developed an artificial intelligence (AI) algorithm that can identify racist code words on social media.\[ But another group of researchers has also shown that Google’s AI tool for spotting online abuse can be deceived. Highly ‘toxic’ phrases can be subtly modified so that the system assigns a lower toxicity score to them.\]

Governments expressed dissatisfaction with the ICANN Board’s decision to allow the registration of two-letter domain names – including country codes – in new gTLDs, over fears that this would create confusion.\[ The Board has been advised to find a solution to meet these concerns.\] Meanwhile, registries of new gTLDs have asked ICANN for a temporary offset of registry fixed fees, given that a number of gTLD operators are struggling.\[ Starting in June, US telecom company Verizon will stop issuing new public static IPv4 addresses, due to a shortage in available addresses.\] ICANN has launched a testing platform in preparation for the root zone DNSSEC key signing key rollover, scheduled for 11 October 2017. DNSSEC is the protocol upgrade that ‘digitally signs’ domain names to prevent their misuse.

Over 170 groups representing consumers, content creators, and civil rights advocates, have urged the US Federal Communications Commission (FCC) and the US Senate Committee on Commerce, Science and Transportation to oppose legislation and regulatory actions that would threaten net neutrality and roll back the important protections put in place by the FCC in 2015.\[ Swedish telecom company Telia Sweden announced that it will be extending its controversial zero-rating services.\] This came after the Swedish Post and Telecom Authority’s announcement that it will make net neutrality a priority in 2017.\[ T-Mobile Netherlands will defend its zero-rating music streaming service in court, opposing a decision by the Dutch telecom regulatory authority which declared the service to be in breach of net neutrality rules.\]

Net neutrality debates are expected in South Korea, after SK Telecom introduced zero-rating for Pokemon Go.\[ Security experts are expecting an increase in cyberattacks on the industrial IoT in 2017. The study by Tripwire Inc, which looked at industrial IoT deployment in organisations, revealed that 51% of the surveyed security professionals do not feel prepared for security attacks.\]

Researchers at the University of Rochester have developed an artificial intelligence (AI) algorithm that can identify racist code words on social media.\[ But another group of researchers has also shown that Google’s AI tool for spotting online abuse can be deceived. Highly ‘toxic’ phrases can be subtly modified so that the system assigns a lower toxicity score to them.\]

Infrastructure

Net neutrality

New technologies (IoT, AI, etc.)
HRC 34TH SESSION: DIGITAL RIGHTS IN GENERAL, PRIVACY IN PARTICULAR

A year after the first report of the United Nations Special Rapporteur on the right to privacy national and international governmental surveillance activities remain in focus in the second report.

The report of UN Special Rapporteur Joseph Cannataci, which addressed the right to privacy, was submitted to the 34th session of the UN Human Rights Council (HRC), held from 27 February to 24 March 2017 in Geneva. During the same session, the UN HRC adopted the Resolution on the right to privacy in the digital age.

The report has two main highlights. The first is that there were no improvements in the status of the right to privacy with a focus on surveillance in the past year. Any legislation that was introduced was either rushed to legitimise practices, or carried only minor improvements.

The second is the Special Rapporteur’s recommendation for a legal instrument regulating surveillance in cyberspace, which came a day after the WikiLeaks Vault 7 leak.

Cannataci’s report directly refers to the Snowden revelations and their aftermath with regard to transparency and remedy, stating that they ‘have clearly shown that there is a pressing need for government authorities to explain their work.’

A legal instrument to regulate surveillance

The proposed legal instrument would grant the equivalent of an international surveillance warrant to address the problem of thousands of requests, which big companies, such as Apple, Twitter, and Google, receive from governments worldwide.

The legal instrument regulating surveillance would complement existing instruments (such as the Cybercrime Convention), or proposed instruments (such as Microsoft’s proposed Digital Geneva Convention). Noting that a pre-existing initiative – the MAPPING project – is already exploring options for such a legal instrument, the Special Rapporteur believes that newly created mechanisms could grow to provide critical mass to a much-needed instrument, as was the experience with other international norms.

Conclusions and recommendations

The report provides five distinct recommendations that deal with:

(a) WHY populism and privacy are inimical to security;
(b) HOW states may engage to improve privacy protection through better oversight of intelligence;
(c) WHY derogations from international norms are unacceptable;
(d) HOW this right to privacy could possibly be better protected through developments in domestic and international law and
(e) WHEN some developments in international law, especially those concerning a legal instrument regulating surveillance may possibly soon be at a stage of maturity where they could benefit from a wider discussion.

In his report, Cannataci finds that ‘extremely privacy-intrusive measures that have been introduced by new surveillance laws in France, Germany, the UK, and the USA’ are dominantly based on the politics of fear, and not on evidence. He invited UN member states to engage in a discussion of the implications of their decisions.

HRC adopts new resolution on the right to privacy

The new resolution adopted by the HRC reinforces certain elements from previous UN resolutions. These include anonymity and encryption, (technical solutions to secure the confidentiality of digital communications are emphasised as important for the enjoyment of human rights); metadata, which can reveal personal information that can be no less sensitive than the actual content of communications; and profiling and algorithms concerns, which can lead to discrimination or decisions that otherwise have the potential to affect the enjoyment of human rights.

On the other hand, for the first time, the HRC resolution emphasises that states should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity, and proportionality.

Looking towards 2018

As a solution, new international mechanisms are recommended, including ‘...executive branches of government to be given a mandate by their parliaments [...] to actively explore such options for proper regulation of surveillance and the introduction of privacy-friendly safeguards and remedies in cyberspace’. He also recommends that judges receive training and support to help them understand the technological implications of their decisions.

Focusing on next steps, the resolution recommends several steps to be undertaken before the 39th Session in September 2018. It invites the convening of an expert workshop on the right to privacy in the digital age, it puts the roles and responsibilities of the businesses sectors in focus, and it calls for a further report of the UN High Commissioner for Human Rights.

The participation of different stakeholder groups was recognised as helpful to better understanding applicable norms on the right to privacy and challenges related to implementation. Cannataci’s report envisages a further set of recommendations in 2018 to ensure the promotion and protection of privacy, including in connection with the challenges arising from new technologies.
IN FOCUS

SHARING ECONOMY: RAPID EXPANSION, RISE IN LEGAL ISSUES

The development of new business models on the Internet, especially those related to the so-called sharing economy, has been accompanied by a rising number of legal and regulatory issues that threaten to jeopardise the business models’ existence.

Uber, the ride-sharing application which has seen a rapid expansion in the past three years, is at the centre of legal controversies related to the sharing economy. This has led to numerous court cases, rulings by regulatory authorities, and decisions by other administrative bodies, in different countries.

In March, for example, the Canadian government decided to amend its taxation laws and redefine ride-sharing firms as taxi companies, ending the tax advantages that they have over traditional taxi companies. In Denmark, Uber will pull out of the country from mid-April, due to proposed regulations that would introduce additional requirements, such as mandatory fare meters and seat sensors.

Most issues associated with the sharing economy are related to the fact that the sharing economy’s business model is still not clearly regulated.

In expanding its business, Uber presented serious competition to traditional taxi services. Many of the initial cases against the company were initiated by taxi associations on unfair competition grounds. The key question is related to how Uber is classified within the scope of the regulatory regime. Is it a traditional taxi service, or an information society service?

This is also on the radar of the Court of the Justice of the European Union (CJEU), after a Spanish judge referred the case to the CJEU in July 2015, asking ‘... whether the firm (Uber) should be considered as a transport service provider or a digital platform’. The classification of Uber, and the status of the sharing economy in general, will depend – to a large extent – on the outcome of this decision.

Courts of various instances were faced with other related legal issues. Among these is the question of whether Uber’s drivers are direct employees or independent contractors. If they are employees, the company needs to provide them with employee benefits, such as social security. The UK courts have already taken a stand, in that drivers are considered to be employees. In the USA, the question is still pending.

Moreover, the lack of licences, safety considerations, and the non-fulfilment of other conditions that are generally necessary for taxi drivers (such as the type of car being used, insurance requirements, etc.) have been raised in other court cases.

In the USA, which has the largest number of cases and class actions against Uber on record, the situation is even more complex due to procedural issues. Numerous disputes are awaiting a final decision on whether drivers can sue Uber in a court of law, or whether they need to resort to arbitration, since drivers’ contracts contain an arbitration clause to which drivers would have agreed before joining the company as service providers.

Uber’s enormous exposure to litigation has triggered a chain of other cases. Among related issues are background checks for drivers, reports to regulatory authorities, the alleged drivers’ discrimination against blind people, and physical assault of customers.

The lack of a clearly defined regulatory regime is perhaps the main reason for so many court cases. At the same time, legal loopholes are a motivation for some to exploit the situation through endless litigation for profit-making. That is why the international community should promptly react in creating a predictable legal framework for the sharing economy that will, at the same time, respect the interests of traditional professions as well as stimulate the digital economy and new business models.

Mapping Uber is an interactive study of court cases and other rulings involving Uber, available at dig.watch/uber. The study analyses 53 cases in more than 25 countries. Visit the dedicated page to read more about each case.
Data is at the core of modern society, from our digital footprint via e-mail and social media, to big data analytics. Artificial intelligence further increases the relevance of data. Cross-border data flows are challenged by policy decisions. How is data shaping our future? How are Geneva-based organisations using data? These and other questions will be the focus of Digital Geneva 2017.

In Geneva, the main operational hub of the United Nations and the international system, data appears in two major realms. First, data is a tool used to develop better policies on health, trade, migration, and climate, to name just a few. Many organisations in Geneva are using data as a tool for research, evidence-based policy-making, and other policy activities. For example, CERN – the European Organization for Nuclear Research – is one of the biggest data processing set-ups globally. Its Data Centre stores more than 30 petabytes of data every year from experiments at the Large Hadron Collider. The United Nations Office in Geneva hosts gvadata.ch, an online space for sharing data related to the sustainable development goals (SDGs).

Second, data is a topic of diplomatic negotiations addressing privacy, security, digital trade, and other important issues. Data as a governance topic is being addressed by many organisations in Geneva. In the area of technology, for example, the ITU, the International Organisation for Standardization (ISO), the International Electrotechnical Commission (IEC), CERN, and other organisations develop the standards and the infrastructure needed for the data-driven era. Issues related to data and trade are addressed at the World Trade Organization (WTO), the UNECE, and the United Nations Conference on Trade and Development (UNCTAD), among others.

**ACTIVITIES AND EVENTS IN 2017**

Digital Geneva 2017, a Geneva Internet Platform initiative, includes a series of activities and events throughout the year, leading up to the 12th IGF meeting.

**Research on data and digital policy:** How does data intersect with digital policy? We look at the role, impact, and relevance of data in areas such as privacy, security, and capacity development.

**Research project on data diplomacy:** An ongoing project, commissioned by the Finnish Ministry of Foreign Affairs, will contribute towards a discussion on the use of data by diplomatic services and international organisations. Join the Roundtable on Data Diplomacy on 5 April.

**Event reports:** Data is the subject of many global and regional discussions. The GIP will report from the main events.

**Monthly briefings:** Data is at the centre of the GIP’s monthly briefings on digital policy. Together with the monthly newsletter, the briefings summarise the main developments in the field.

**Luncheon discussions:** Regular discussions in Geneva will gather practitioners to brainstorm data as a tool and to share best practices. Contact us (gip@diplomacy.edu) to join.

**Workshops at main digital policy events:** The GIP and DiploFoundation will host workshops at main events including RightsCon, EuroDIG, the WSIS Forum, and IGF 2017. Follow updates.