IEEE

EU Policy News Bulletin

ICT

June 2017

AT A GLANCE: BREXIT GUIDE ON ICT NEGOTIATIONS – GOVERNMENTS SCRAMBLE TO RESPOND TO GLOBAL CYBERATTACK – FACEBOOK USES ARTIFICIAL INTELLIGENCE FOR COUNTERTERRORISM

TABLE OF CONTENTS:

BREXIT

Guide on ICT talks

Brexit talks are now finally underway. This month the EU and U.K. teams met with an exchange of gifts and an agreement on how the talks would proceed. The U.K. made a significant concession by agreeing to talk about what the EU wants to talk about (the terms of the divorce) before moving on to what it wants to talk about (trade and the future relationship between the two sides).

One key issue that had to be tackled early on was settling the U.K.'s financial obligations to the rest of the bloc — the so-called Brexit bill. That impacts on everything else because the EU27 says they are not willing to move on to other things. Here's a guide to what is at stake in the area of ICT once the financial discussions are out of the way:

- What's at stake? If London wants to keep its top reputation for start-ups and data innovation, it will have to negotiate ways to transfer data smoothly to and from the EU. The country's invasive surveillance practices could stand in the way of that. Migration is also high on the agenda for techies, who fear a brain drain of coders and entrepreneurs. The EU, on the other hand, stands to lose a tech-savvy member with the skills and pro-business agenda the Commission likes.
- What's not? The digital economy — everyone loves the digital economy.
- Biggest potential losers: Start-ups in London; research departments across Europe.
- Biggest potential winners: Privacy advocates; EU countries that take up Britain's lead role on tech.
- Key decision: Whether a data transfer deal is struck.
- Key person on U.K. side: Gila Sacks, director for digital and tech policy at the U.K.'s department of culture, media and sports, will support the DExEU team with expertise.
- Key person on Brussels side: François Arbault, key person in charge of internal market and sectoral policies.

Source: Politico Pro

DIGITAL ECONOMY & SOCIETY

Mariya Gabriel new Commissioner for Digital Economy and Society

Mariya Gabriel, currently a Bulgarian MEP for the EPP group, was nominated by Commission President Jean-Claude Juncker to take over the responsibility for the Digital Economy and Society portfolio.

The Industry and Research Committee and the Culture and Education Committee held a hearing with the candidate commissioner on 20 June. Following the evaluation of the committees' coordinators, the Conference of Committee Chairs and the Conference of Presidents decided to close the hearing.

Parliament will now have to back the appointment of Ms Mariya Gabriel at the plenary meeting in July.

The Commissioner for the Digital Economy and Society will support the implementation of the Digital Single Market Strategy. She will contribute to delivering a Digital Single Market, helping to lay the groundwork for Europe's digital future with EU-wide telecommunications networks, digital services that cross borders and a wave of innovative European start-ups. She should also ensure that the right conditions are set, including through copyright law, to support cultural and creative industries and maximise their potential for the economy.

Source: Dods

Q and A with Estonian presidency digital expert Luukas Ilves

Estonia wants to set an e-example for Europe. Digital will be a running theme throughout Estonia's presidency of the Council of the EU, which will start on 1 July. The country plans to launch a virtual reality hub in the Council building in Brussels, put self-driving buses on the streets of Estonia's capital Tallinn and organized a special Digital Summit with EU leaders.

But what can this e-presidency hope to achieve?

In an interview with Politico, Luukas Ilves, the Estonian permanent representation's counselor for digital affairs, explains Estonia's digital priorities and how these overlap with the Commission's digital single market strategy.

Ilves says the presidency hopes to make progress on the European Electronic Communications Code, copyright, the free flow of data and cybersecurity. He also emphasizes the need for closer cooperation with the Commission, particularly on security issues.

What themes will you explore during your presidency?

The general chapeau we have is the free movement of data. We really think of that in a broad sense. It isn't specifically about [the Commission's initiative on the free flow of data. Not having geo-blocking is free movement of data, having Gigabit internet is free movement of data. It's a political goal. We want to put it on the table to see if it makes sense to look at the free movement of data as something longer-term in the same way as we have with the existing four freedoms. We'll see how much traction that gets.

Which policy files will top the priority list?

The two toughest files, that we have to do a lot of work on but that we're not going to deliver a conclusion on, are clearly copyright and telecoms [reform]. A lot of the low-hanging fruit from the [digital single market strategy] has now been picked, and we have the tough, difficult files.

How are you dealing with the issues surrounding the telecoms proposal? There has been a lot of pushback from member countries.

Right now, it's a bit of a red herring to focus just on the [European Electronic Communications] Code. Is the 5G rollout that's supposed to happen over the next few years going to happen as quickly, as thoroughly and as consistently across Europe as it could? One of the things we will be doing in parallel to the negotiations of the code is to say, "*Ok, let's talk about what we can actually do with the existing mechanisms.*" The code is not going to be law for a few more years because of transposition deadlines. What member states have all said in the past on these negotiations is, "*Look, we have the legal toolbox that we need already so we don't need further formal legal coordination.*"

Tell us how the presidency is working with Digital Vice President Andrus Ansip's cabinet and the Commission? Clearly you have strong connections [since Ansip is the Estonian commissioner].

There's a lot [of cooperation.] We definitely keep each other closely apprised of what we're working on. What is clear is that, given how quickly things are moving in cyber, it's really important to have open-minded communication and not just rely on the formal processes. [The Commission plans to release their renewed cybersecurity strategy in the fall.]

We've seen in previous negotiations on cyber that … the Commission is a black box and they put their proposal on the table, then the member states are locked out. We saw this on the Directive on Security of Network and Information Systems, [which came into force last year.] There were really strong red lines on national security and sovereignty that maybe could've been overcome. What that really requires is for member states to have a hand in the nuances of how a mechanism gets designed.

One of the EU's biggest problems is failing to translate its achievements into a real-world context. Is there one file that could be the new roaming?

I'll be honest, I think we're playing a long game here. I would say that a lot of what we want to accomplish is feel-good digital. I mean, look, [telecoms] access regulation will be boring regardless. We would say that all the stuff on e-government is ultimately a feel-good thing but, on the other hand, doing the underlying work, building up electronic identity infrastructure in a country, for example, doesn't happen overnight.

Source: Politico Pro

CYBERSECURITY

Governments scramble to respond to global cyberattack

Last month a second outbreak of ransomware in less than two months highlights how vulnerable Europe remains to cyberattacks, despite repeated commitments by officials to boost cybersecurity.

Security experts were working around the clock to analyze the ransomware — dubbed *NotPetya* for its similarities to a previous attack — which disrupted Kiev's airport along with banks, transport networks and energy supplies across Europe.

The ransomware hit computer systems in at least 65 countries, according to Microsoft. Ukraine was most severely affected but the malware also spread in Germany, Russia, the United States, the United Kingdom and across the globe.

Organizations that had to partially shut down included Russian energy firm Rosneft, Ukrainian energy firms Ukrenergo and Kyivenergo, Danish transport company Maersk, U.S. pharmaceutical firm Merck and parts of the Ukrainian government. Even some computers in the Chernobyl nuclear facility were infected.

The attack comes just weeks after the similar "WannaCry" crisis crippled hundreds of thousands of computers globally in May.

"*If WannaCry was a viral cold/influenza, the current attack is like a severe disease spreading at a much slower pace, the virus is more disruptive but the damage affects less people*," said one European security official, speaking on condition of anonymity.

At the European Commission, spokesperson Margaritis Schinas said the

latest attacks "*show we need more awareness about cyberthreats and more action by all actors involved.*"

The trouble is that governments and lawmakers remain puzzled over how to prevent such attacks.

The European Union last year adopted its first piece of hard legislation on cybersecurity. The "Network Information Security Directive" aims to secure "critical infrastructure" such as energy and transport networks, banking and health care IT.

In past years, governments across Europe have set up cybersecurity centers to help fight cybercrime and hackers attacking their systems. The NIS Directive asks them to draft a strategy, too, to figure out how to respond to cyberthreats.

So far, progress has been slow, and some have questioned how serious EU countries are about making sure the Commission's recommendations are implemented. "*The question is whether people will do genuine and serious enforcement,*" said Ilias Chantzos, senior director for government affairs at cyberfirm Symantec.

Other experts point out that governments don't always provide strong examples when it comes to cybersecurity, which requires, among other things, ensuring software remains up to date.

This week, reports showed the U.K.'s largest warship runs the Windows XP operating system, software that hasn't been supported by Microsoft for years. Belgian police have complained of having to fight a growing terrorism problem with outdated IT. London's Metropolitan Police struggles with the same issue. The European Parliament recently switched from Windows XP to Windows 7 — an operating system that dates back to 2009.

Most European governments are in the first stage of protecting themselves from hackers, Eugene Kaspersky, founder of the global cyberfirm, said in a recent interview. "*They have a definition of the critical infrastructure, a definition of the tools*," he said. "*But they still need to protect the systems and then to implement it.*"

That's the hard part, he added.

"*A lot of these attacks really require training [to prevent]*," said James Norton, a cybersecurity consultant and former deputy assistant secretary at the U.S. Department of Homeland Security. Few companies and governments, he added, invest in the necessary training.

On Wednesday, security experts were still looking for the mastermind behind the NotPetya attack. There were some indications that the malware had targeted Ukrainian networks — but none could say with certainty who did it.

In the case of the WannaCry outbreak last month, some firms and, reportedly, the U.S. National Security Agency, linked the malware to the North Korean government.

Since Petya caused the most damage in Ukraine, researchers are looking at potential links to Russia.

Some have raised question over whether the malware, which asked for $300 in exchange for decrypting the files on infected computers, was meant to make money at all.

"*We're trying to figure out how targeted it is, or not*," said an employee at a global cybersecurity firm who asked not to be named because the investigation was ongoing. "*You'd imagine this to pop up in places where people have $300*," the source said. "*Ukraine doesn't come to mind.*"

Source: Politico Pro

DATA PROTECTION

Data protection watchdogs pressure Commission on privacy shield

European data protection watchdogs asked the European Commission to take a stronger stance toward the U.S. on privacy protections.

The Article 29 Working Party of data protection authorities sent a letter to the Commission outlining what they want to see in the EU-U.S. data transfer deal "privacy shield."

Watchdogs want "precise evidence" on how the U.S. intelligence services gather data, and an explanation from U.S. authorities on when the Trump administration will fill vacant positions of officials in charge of EU citizens' data protections, it said in a press release.

The privacy shield deal was struck a year ago and will be discussed when the Commission visits Washington in September.

The data protection authorities' request clashes with the Commission's plan for the privacy shield's first annual review, which the Commission has said will focus on minimizing any deterioration in protections. Getting more privacy protections "is not our starting position," a high-level Commission official said in May.

Source: Politico Pro

Parliament lights privacy fire in draft e-Privacy report

The European Parliament's rapporteur for the draft e-Privacy Regulation raised the stakes on privacy rules for electronic communications, in her **draft report** published.

Marju Lauristin, the Estonian MEP tasked with guiding the bill through

Parliament, published her draft report after weeks of hearings on how telecoms and communication applications like Skype and WhatsApp should protect people's texts and calls.

The draft shows Parliament will push for a number of privacy-enhancing elements in the bill when it negotiates with EU countries later this year.

Among the amendments Lauristin suggested, one would ban websites like Facebook from refusing people a service if they don't consent to sharing personal data beyond what's strictly "necessary for the provision of that service." In effect, it could kill free services that monetize personal data.

Another change makes "Do Not Track," a mechanism in which internet users' choose to reject cookies that track their browsing, legally enforceable against websites that do not respect it.

The draft also strengthens protections for encrypted communications and against tracking on Wi-Fi networks and in closed "intranet" networks.

It introduces a stricter requirement for software developers to make their default settings as privacy-friendly as possible, something known as "privacy by default."

These points, when passed by fellow MEPs, would make negotiations with national governments harder in the fall. The EU aims to have a final e-Privacy Regulation in place by May 2018.

Source:

AI & ROBOTICS

Facebook says it uses artificial intelligence, partnerships, staff for counterterrorism

In a blogpost published earlier this month, Facebook states it is using artificial intelligence, staff members and partnerships to monitor its 2 billion active members, as part of its counterterrorism strategy in response to questions about its role in fighting terrorism.

Facebook outlined five artificial intelligence practices it has incorporated, including image matching and language understanding. The blog said the company's use of artificial intelligence to watch for terrorism is "fairly recent."

"*We're constantly identifying new ways that terrorist actors try to circumvent our systems — and we update our tactics accordingly*," Facebook officials Monika Bickert and Brian Fishman wrote in the blog post.

Bickert and Fishman said Facebook employs 150 staff members focused primarily or exclusively on counterterrorism, and it reviews material reported by users.

The company said it is also using partnerships with other companies, including Twitter and Microsoft, and other programs, as part of its effort.

"*The challenge for online communities is the same as it is for real world communities — to get better at spotting the early signals before it's too late*," the blog post said.

Source: Politico Pro