CAB GABRIEL/662
Meeting with [redacted] Symantec
05/09/2018

Scene setter

You will meet [redacted] Symantec on 5 September 2018, 14:30. [redacted] is likely to raise issues about the Cybersecurity Package and the ePrivacy Regulation.

About Symantec

Symantec is an American software company founded in 1982 and headquartered in Mountain View, California. The company provides cybersecurity software and services, and offers professional services to support its software. It is a global leader in cybersecurity.

Cybersecurity

Symantec's position on the Proposed Cybersecurity Act

Symantec is a member of the BSA – Business Software Alliance which has produced a position paper regarding the proposed Cybersecurity Act. Overall, it welcomes the suggested changes. Some concerns expressed are related to the following:

1) Alignment with existing international standards

"[S]*chemes should, by default, identify and align with an existing international standard,* *such as the ISO 27000 series, and conform to international best practices (such as those reflected in the ISO/IEC CASCO Guidelines)..... In those instances where ENISA seeks to deviate from existing international standards, they should be* ***required to request a "waiver"*** *with a clear explanation as to why international standards are not sufficient. The* ***European Commission be required to consult in advance with industry"***

2) Stakeholders involvement in relation to proposing and designing schemes

"We encourage policymakers, particularly the European Commission, to create a clear "roadmap" and ***procedure to formalise consultation with stakeholders prior to issuing a request for ENISA to begin working on candidate schemes.*** *This could be achieved by introducing (e.g., in Article 44) a means for ENISA's "Permanent Stakeholder Group" to suggest new schemes, and giving it a specific and meaningful role during each scheme's creation. This should be in addition to the possibility for industry to propose to the European Commission to consider approving an industry certification scheme as a European scheme (Recital 53)."*

3) Updates should not automatically trigger a requirement to re-certify

"*The future framework should make clear that updates should not automatically trigger a requirement to re-certify. Instead, all schemes should provide a "light touch" (e.g. automatic, cost-free renewal following attestation from the certificate-holder that there have been no material adverse changes to the security of the product or service) process to assess the impact, if any, of relevant updates on the conformity of the certified ICT product or service with the certification requirements."*

4) Self-certification for "low-risk" technologies

"The Regulation should explicitly call out self-certification and self-declaration as viable options. We encourage the co-legislators to introduce into the text a ***tiered approached, based on risk profile, whereby there wold be an option for self-assessment for technologies deemed as low-risk."***

ePrivacy

Symantec's position on the Proposal for an ePrivacy Regulation

In general, Symantec supports the stated objectives of the draft ePrivacy Regulation.

Article 6 of the draft ePR allows electronic communication services ("ECS") and electronic network providers ("ECN") to invoke exceptions to process electronic communications data. However, as Symantec's own security service that processes communications metadata on behalf of an end-user (e.g., a bank or a website provider) may not be classified as ECS or ECN, Symantec may be unable to benefit from the exceptions found in article 6. The Software Alliance, from which Symantec is a member, therefore recommends to broaden the scope of Article 6 so that the exceptions are not only available to ECSs and ECNs, but to all other parties (i.e. end-users) that are subject to the prohibition in Article 5.

Furthermore, Symantec supports the proposed amendments to **recital 8** put forth by the Bulgarian presidency in its recent paper dated 4 May, however would prefer to have them in the Article: *"Some end-users, for example payment service providers and payment systems, process as recipients their electronic communications data for different purposes or permit other parties to process their data on their behalf. Such processing may include the processing by an information society provider, or another party on its behalf, for purposes such as ensuring network and information security, including the prevention, monitoring and termination of fraud, unauthorised access and Distributed Denial of Service attacks, or facilitating efficient delivery of website content. Such processing is not covered by this Regulation."*

Position of the Commission

In the view of the Commssion, broadening the scope of article 6 would be problematic. The commission considers that Symantec does not fall within scope of the ePR and therefore does not see a reason to cater for an exception for security service providers.

Recital 53 of the current Directive (as reviewed in 2009) and Recital 49 of the GDPR, which mirrors this, clarifies that the processing of metadata by an end-user or a security company contracted by the end-user is covered by the GDPR. The Commission sees as such clarification in the Recital is sufficient, as it was already sufficient having this recital in the GDPR, taking into account that ePrivacy Regulation is a *lex specialis* to the GDPR.

Moreover, the proposal of Symantec to broaden the scope of Article 6 would be problematic as this would allow them to process the electronic communications data of all end-users for security purposes, irrespective whether they have a contract with them or whether the end-user has requested to do so. Thus, a permission to this end would put at risk the confidentiality of communications.

Line to take

Cybersecurity Act

The European Cybersecurity Certification Framework

- The "Cybersecurity Act", including an ICT cybersecurity certification framework, addresses very well these concerns and will allow for the definition of appropriate cybersecurity schemes for consumer IoT products and services, among others
- We have therefore put forward a proposal for a European cybersecurity certification framework that:
  - Will help **to reduce fragmentation** in the single market due to divergent national schemes but also provide the right governance framework to establish certification schemes tailored to different needs.
  - is flexible **to address the needs of the entire DSM**; from high to low risk, from critical infrastructures to individual citizens,
  - builds upon and fully embraces **the successful schemes that are now in place** (e.g. SOGIS-MRA)
  - is forward looking in order **to address the Union's future needs** both in the short and also long term.
- The Certification Schemes will be voluntary but they may be used by legislators in future sector or product specific regulation.
- The Joint Communication has already hinted at priority areas such as:
  - Security in critical or **high-risk applications** (from airplanes or power plants to the smallest such as medical devices).
  - **Widely-deployed** digital products, networks, systems and services used by private and public sector – such as email encryption, firewalls and Virtual Private Networks;
  - The use of **"security by design"** methods in low-cost, digital, interconnected mass consumer devices which make up the Internet of Things: schemes under the framework could be used to signal that the products have undergone adequate security testing.

The Competence and Research Centre

- It is in the EU's strategic interest to ensure that the EU retains and develops the essential capacities to secure its digital economy, society and democracy, to protect critical hardware and software and to provide key cybersecurity services.
- The Public-Private Partnership on Cybersecurity created in 2016 was an important first step, triggering up to EUR 1.8 billion of investment by 2020.
- However, the scale of the investment under way in other parts of the world (e.g. the US will invest 19 billion dollars in cybersecurity in 2017 alone although not only in Research and Innovation) shows that the EU needs to do more to achieve a

critical mass of investment, and to overcome the fragmentation of capacities spread across the EU.

- The EU needs now to give impetus to our innovation and competitiveness in cybersecurity. In this line, the Commission aims to boost efforts for the EU industry to be on the global scene in the development of the next-generation cybersecurity and digital technologies such as artificial intelligence, quantum computing, block chain as well as boost digital skills.

- In this context – To put efforts and capitalize our synergies, we propose to establish a Network of cybersecurity competence centres with a European Cybersecurity Research and Competence Centre at its heart. Commission notices the high interest of research for funding, and there is a real need to encourage investments to commit a common engagement in fostering research and innovation.

- The Commission also proposes to launch a pilot phase under Horizon2020 in order to create a new momentum in cybersecurity investment. The Commission plans to make available €50 million in funding in the short term for this.

ePrivacy Regulation

- The objective of the proposed Regulation on Privacy and Electronic Communications published in January 2017 is to complement the General Data Protection Regulation (GDPR) with rules appropriate for the electronic communications sector – resulting in more specificity, harmonisation and a high level of protection.

- While the General Data Protection Regulation applies to personal data, the ePrivacy proposal protects confidentiality of communications as such, independently of whether personal data is involved. It protects information that pertains to legal persons, not only to natural persons. This is relevant to guarantee the secrecy of communications and protect business information.

- The security of network and processed data is of utmost importance to ensure confidentiality of communications.

- As regards market operators, existing European legislation such as the NIS Directive, the General Data Protection Regulation, the proposed Electronic Communication Code and the ePrivacy Regulation (the last two under negotiations), all place obligations on markets operators to take reasonable (cyber)security measures in order to protect the services they offer or, in the case of the GDPR, the personal data of their customers and employees, from (cyber)security threats.

- As regards your concern, the processing of incoming traffic is covered by the GDPR. Recital 49 of the GDPR specifies it. It means that for instance a bank or other company is allowed to process incoming traffic for the security purposes, to protect their systems and websites. They can do so and Recital 49 of the GDPR clarifies that it should be seen as their legitimate interest. An end-user can also contract a security company to do it for them.

- This is also clear from the ePrivacy proposal, were it is clarified that the processing of communications data that were received by recipients of these communications is covered by the GDPR (not by the ePrivacy Regulation).

- As we believed that Recital 49 of the GDPR is sufficient to clarify the situation; the Commission did not copy it in the proposal. It is worth noted that the Council's recent draft text includes caters for the requested clarification that security companies acting on behalf of an end-user do not fall under the ePR (Recital 8). The co-legislator could further elaborate on this if deemed necessary.

Defensive points

Cybersecurity

Will the European framework fit into existing or international initiatives?

The rules on cybersecurity certification provide a tool for companies subject to the NIS Directive, as they would have the opportunity to procure certified ICT products and services on the basis of cybersecurity certification schemes valid and recognised throughout the EU.

The framework itself is without prejudice to existing harmonised legislation such as the Radio Equipment Directive or other legislation such as eIDAS or the GDPR.

As regards international initiatives, the schemes proposed in the future European framework will rely as much as possible on international standards and ensure coherence with international initiatives. For example, the European framework will take into account the current achievements of the SOGIS-MRA community. In addition, the creation of the European Cyber-Certification Group (ECCG) composed of national representatives will promote the formation of a common position among those Member States participating in international fora such as the Common Criteria Recognition Arrangement (CCRA). The Group (ECCG) will also advise the Commission on the extent to which international initiatives are appropriate to satisfy security needs in the EU.

Which standards/technical requirements will the EU certification schemes be based on? How will potential obsolescence be prevented? How will they be designed to prevent that they hinder innovation?

Individual EU certification schemes will specify the standard or technical requirements it relies on. In many instances these will be existing European or international standards such as those used in the current SOGIS-MRA. With regard to obsolescence and innovation, the cooperation between ENISA and standardisation bodies will enable to monitor the appropriateness of standards used in a European scheme so that they ensure an adequate level of both security and technological innovation. Such a monitoring exercise will mitigate the risks related to the obsolescence of standards that may provide buyers with a false sense of security.

Can SOG-IS MRA be integrated into the proposed framework?

Yes, our framework would allow building a dedicated scheme that replicates the features of the current SOGIS-MRA. Such a possibility would turn the current SOG-IS MRA into a fully-fledged European scheme.

The SOGIS-MRA is a certification scheme albeit not a pan-European one (i.e. not all Member States participate). It is also a "governance" model whereby specific Member State authorities (e.g. ANSSI, BSI and other participant authorities) cooperate and jointly "govern" cybersecurity certification.

Our proposed framework has been inspired by the governance model of SOGIS-MRA.

For example, we propose the creation of the ECCG (Article 53) which brings together National certification supervisory authorities (Article 50).

We have also specific provisions that allow Certification Authorities to issue certificates and, very important, supervise the private conformity assessment bodies undertaking the evaluation (Article 50 6 (b).

What standards or technical regulations will be adopted in the future for cybersecurity certification? Will new standards or technical regulations be developed for cybersecurity certification of ICT products and services because of this proposal?

The proposal does not foresee the adoption of standards or technical regulations. The aim is to make full use of existing standards. The application of the schemes is voluntary. If there is a clear need for any new standard to be developed, this will take place within the standardisation organisations.

Would a certification scheme focus on products specifically, or on processes?

The Regulation refers to products and services. However, it is possible that a scheme – especially if tailored for high level certification - includes requirements on the development and other life-cycle related processes. These requirements may be placed on top of product-specific ones.

What is the role of industry in the framework?

Industry plays an important role in the Cybersecurity Certification Framework.

First, the schemes rely on standards and industry's role in standardisation of course central.

Second, when ENISA prepares a candidate scheme, the regulation clearly states that it "shall consult all relevant stakeholders" which includes industry – both the vendors and the users of ICT products and services.

Finally, the schemes will be established by implementing acts which themselves are subject to public consultation.

Will the process of developing the cybersecurity certification system by ENISA be open and transparent? How could foreign stakeholders participate in the development process?

Yes. The process by ENISA will be open and transparent. Foreign stakeholders, namely industry, can participate in ENISA's consultation as well as their work and contributions to the work of standardisation bodies.

How does the framework address the issue of re-certification or software update

Specific provisions on re-certification and updates can be considered when determining the elements of the scheme.

Can there be a role for self-certification in the framework?

Certification, as defined by ISO, implies the assessment by an independent third party. In the case of self-attestation or 1st party attestation, a vendor or supplier attests by himself that the product or service meets the requirements of a particular scheme. As such, self-attestation has not been included in our proposal. In our view, in itself self-attestation provides very little, if any, assurance when not coupled with other measures such as market surveillance. Such measures are not yet in place in the sector of ICT.

Why do we need a Research & Competence Centre? Isn't strengthened ENISA enough?

ENISA has a role to play in advising on cybersecurity research and innovation in the EU but its proposed mandate focuses first and foremost on other tasks crucial for strengthening cybersecurity resilience in the EU. The mandate of the European Cybersecurity Research and Competence Centre should be complementary to these efforts but requires different focus and set of skills. The Centre should stimulate development and deployment of technology in cybersecurity and complement the capacity building efforts in this area at EU and national level. The Commission will launch an impact assessment to examine available options – including the possibility of setting up a Joint Undertaking – with a view to set up this structure in 2018. This will also address the synergies with ENISA.

In 2016 you announced cPPP. Why a new project of Competence Centre now?

The Public-Private Partnership on Cybersecurity created in 2016 was an important first step, triggering up to EUR 1.8 billion of investment by 2020. However, the scale of the investment under way in other parts of the world (e.g. the US will invest 19 billion dollars in cybersecurity in 2017 alone) shows that the EU needs to do more to achieve a critical mass of investment, and to overcome the fragmentation of capacities spread across the EU. This activity will complement the ongoing implementation of the Public-Private Partnership on Cybersecurity.

ePrivacy Regulation

Under the ePrivacy Regulation security providing companies will not be able to process incoming traffic data and will not be able to prevent security attacks.

- **This is not correct.** The processing of incoming traffic data is covered by the GDPR. Recital 49 establishes that data controllers, such as web sites as well as security companies acting on behalf of the web site, have a **legitimate interest** to process incoming traffic to secure the web site (prevent unauthorised access).
- Explanation: Under the ePrivacy proposal, the processing of communication data that were received by recipients of these communications is covered by the GDPR as far as it concerns personal data (not by the ePrivacy Regulation). This means that recipients of calls may process the phone numbers; it also means that web sites may process the IP addresses of visitors to the web site. The analysis of IP addresses is an important tool for web site owners to ensure the security of their web sites.
- The application of the GDPR to the analysis made by web site owners also encompasses situations where the web site owner entrusts third parties (like security companies) to do such tasks. For example, if a bank entrusts security company to analyse its incoming traffic data to the bank web site for the purpose of ensuring network security, this processing would be covered by the GDPR, independently of whether it is carried out by the bank or by security company.
- Security companies may also carry out some task on their own initiative. An example would, in simple terms, be a security company sending messages ('pings') to a great number of services, for example to detect whether they would be vulnerable to a certain virus. In case a service responds to the ping, this may be an indication that security measures of the service need to be improved as it may be susceptible to a certain virus or attack. In this example, the security company and service act like communicating parties, with on the one side the security company as the sender, and on the other side the service as the recipient. This means that this activity falls outside the scope of the proposal.

- Furthermore, the GDPR would also apply to a security company that sets forth a so-called honey pot (a honey pot consists of a given web site that appears like legitimate, but in fact is like a trap and serves to analyse traffic to such web site). Last but not least, a telco may also make use of a security company (like Symantec) to analyse traffic data.
- Note that the approach to the GDPR as included in recital 49 GDPR is not new. It was already included in the current ePrivacy Directive (as amended by Directive 2009/136/EC), in recital 53. Such recital was also added to the recent BGP text. As such processing would not be covered by ePrivacy Regulation, there is no need to add the provision to the Article and explanatory Recital is sufficient to ensure legal certainty.
- Some providers seem to have tried to obtained a much wider exception that would give them a blank check to process traffic data under the legitimate interests, almost in a similar way as law enforcement authorities (enabling a security company – on its own merits, not entrusted by a data controller – to police the web and grab traffic data for the purposes of improving its services). Such a provision was not accepted in 2009 (when this debate started), nor in the GDPR and it would be extremely problematic in the ePrivacy Regulation.
- Our recommended LTT is that the GDPR is clear enough. But for more clarity BGP included a similar recital (49) of GDPR or recital 53 of the ePrivacy Directive in their recent text (Recital 8).

Background notes

Cybersecurity

State of play in the legislative process

The negotiations on the Cybersecurity Act started in November 2017 and are proceeding for both co-legislators.

European Parliament:

The ITRE Committee has been appointed as lead Committee. IMCO has shared competence on certification.

The draft report from the rapporteur - Ms Niebler (DE-EPP) - was presented on 26 March. The ITRE Committee (Industry, Research and Energy) has adopted - by a large majority - its report as well as the mandate to start negotiations on 10 July 2018. The Committee mandate to enter into negotiations is expected to be announced at the forthcoming EP plenary on 10 September 2018.

Among the associated committees, LIBE has voted on its report on 8 March, BUDG on 15 May and IMCO on 16 May.

Council

The Bulgarian Presidency, building on the work of the Estonian Presidency, has prepared a compromise text that has been presented and approved at COREPER on 25 May. On this basis, the Bulgarian Presidency reached an agreement on a General Approach at the Telecoms Council of 8th June 2018.

The Austrian Presidency is expected to be ready to start the trialogues as soon as the Parliament is ready (most likely in September).

European Parliament and Council positions

On ENISA, the EP's position is positive overall and ambitious in particular with regard to the Agency's tasks and capabilities related to Operational Cooperation whereas the Council has placed important restrictions to the Agency's objectives and tasks in this area.

On Certification, both co-legislators have overall maintained the Commission's approach for a flexible Cybersecurity Framework and both introduced amendments to allow for schemes based on self-assessment i.e. without third-party certification for low assurance levels.

The EP has however included an amendment for mandatory certification of ICT products and services used by Operators of Essential Services as defined in the NIS Directive. The EP has also introduced additional steps in the scheme preparation phase, which can create important delays. For example, the EP proposed that a formal programming document should be adopted by delegated act before the Commission can request ENISA to prepare any certification scheme.

The Council amendments have also introduced additional steps in the scheme preparation and adoption process (e.g. the Group shall adopt an opinion on the candidate scheme before its submission to the Commission) as well the potential for blocking minority from Member States.

The cumulative effect of these changes can negatively impact on the ability of the framework to deliver schemes in a reasonable timeframe.

In addition, the Council introduced new elements in the cybersecurity certification schemes, such as the inclusion of "ICT processes" in the scope of the schemes, the possibility of a peer review mechanism between national cybersecurity certification authorities and the conditions for mutual recognition of certificates with third country schemes;

ePrivacy Regulation

State of play of the ePrivacy Proposal in the legislative process

The Commission adopted its proposal in January 2017. In October 2017, the **Parliament** gave the mandate to the rapporteur (currently Ms Birgit Sippel (S&D, DE)) that will allow her to start trilogue negotiations. Broadly, the position of the Parliament goes further than the Commission's proposal in terms of protection.

The **Council** has not reached its position yet. The BG Presidency has made considerable progress on the file and adopted a progress report. The AT Presidency now took over the file and the Commission counts on the ATP to bring the file to trilogues. The European Council Conclusions of 28 June 2018 state that "it is vital to deliver on the remaining legislative proposals concerning the DSM before the end of the current legislative cycle".

Curriculum Vitae

[redacted]

[redacted]

Contact(s): [redacted] **(DG CNECT), tel.:** [redacted] **(ePrivacy)**

[redacted] **(DG CNECT), tel.:** [redacted] **(Cybersecurity)**