Tonio Borg: At the EPHA conference, the EU Health Commissioner discussed his growing anxiety over citizens’ wellbeing.

Dacian Cioloș: The outgoing Agriculture Commissioner reflects on his time in Brussels and the increasing contributions of Horizon 2020.

Androulla Vassiliou: Following four years of service, the Commissioner for Education and Culture promotes closer European ties.

CAST OUT
WILL SWITZERLAND SEE A RETURN TO FULL ASSOCIATION STATUS IN HORIZON 2020?
I am pleased to have the opportunity to address you in this foreword to the October 2014 edition of Horizon 2020 Projects: Portal in order to highlight the importance of innovation for industry in the EU. As European Commissioner for Industry and Entrepreneurship, I am committed to giving a fresh impulse to Europe’s ability to lead a new industrial renaissance, through research and innovation. Horizon 2020 is therefore one of our main tools to achieve this objective.

The recent crisis has struck the European economy particularly hard. Europe lost four million jobs in industry and €350bn in investments. However, during these difficult times we have learned that countries with a strong industrial base suffered less. There is now a widespread consensus that such a foundation is vital for the EU’s growth and for job creation. This was underlined in the European Commission’s recent communication calling for an industrial renaissance. On this basis, the European Council acknowledged the central importance of industry and adopted strong conclusions on the way forward. At the request of the Council, I am determined to work during the next months on a detailed roadmap setting out specific actions and measures to be taken in the coming years. This roadmap should be based on four main pillars: access to markets, access to inputs, a business-friendly regulatory framework, and smart industry and innovation.

Despite the progress made so far, there is still a huge potential to strengthen the EU’s internal market by removing the remaining barriers that hamper the competitiveness and growth of business. In parallel, internationalisation and support to European firms’ access to non-EU markets must be made a priority. Particular attention should be given to facilitating access to finance, notably COSME and Horizon 2020. To ensure the competitiveness of our businesses, we also need to reduce administrative burdens and make the economic environment more conducive to business.

In the area of smart industry and innovation, Horizon 2020 has a particularly important role to play. To restore the European economy’s competitiveness, our enterprises need to be able to innovate and rapidly adapt to changing conditions. My overall aim for Horizon 2020, especially through its industrial leadership policy, is to ensure that it prioritises activities targeted at industrial and commercial success, both via the drafting of its work programmes and thanks to a strong focus on close-to-market projects.

I am firmly committed to helping SMEs thrive: they are the backbone of the EU economy and are responsible for the creation of 85% of all new jobs in Europe. The EU’s 20 million SMEs represent 99% of our businesses, and this is why Horizon 2020 provides reinforced support for them, with over 10% of its budget earmarked for SME participation. Horizon 2020 focuses on new forms of innovation and increasing such levels in SMEs. It contains the targeted SME Instrument with a budget of almost €3bn. This instrument aims at helping innovative small companies to obtain funding for market-driven and high-risk research and innovation projects with a clear European dimension. In parallel, stimulating investments in new technologies with a high growth potential, such as Key Enabling Technologies, will also be central to support the industrial renaissance through Horizon 2020.

Over many years, the Commission has developed an extensive network to support SME growth and innovation across the EU, namely the Enterprise Europe Network. Through Horizon 2020, we will be able to pursue activities of the EEN, those that enhance the capacity of SMEs to manage innovation, and those that support cluster activities that foster cross-sectorial and cross-regional links between enterprises.

During my mandate as European Commissioner, I intend to use these strategies to contribute to Horizon 2020’s goals of speeding up the development of technologies and innovations that will underpin tomorrow’s businesses, and help innovative European SMEs to grow into world-leading companies.

To conclude, I cannot but underline that we will never achieve these objectives alone, without your support of, and participation in, the new framework programme. This is why I invite all of you to seize as many opportunities as possible that will be offered by the EU thanks to Horizon 2020.

Opinions here are only those of the author and do not represent the views of the European Commission.
sensitive data according to the minimality principle. It states that sensitive data should be controlled by the user during its whole lifecycle and disclosed to the lowest possible extent for a minimum period of time only to entities and for purposes authorised by the user. This means that, ideally, the minimality principle should guide the balance between data disclosure and usability, but in practice this is rarely the case.

A reason for this is the massive user profiling by online service providers. User data has market value, whereas the surveillance and lawful interception by government agencies and law enforcement authorities help detect and monitor social threats, and detect, track and investigate criminal or terrorist activities. The position of the PST AL is that the minimality principle should explicitly be supported by appropriate regulation at the EU level, especially with respect to user profiling and lawful interception. In particular, instead of the current practice with privacy policies essentially being out of control of the user, we suggest that the online service providers could use self-certified or certified privacy assurance levels. We also wish to raise social awareness about the need for, and the value of, data security and privacy in a digital society and encourage the corresponding top-down initiatives and approaches.

Defensive techniques

Traditionally, cybersecurity has been respectively related to the offensive or defensive techniques that can be used for performing attacks or defences against the attacks in cyberspace.
Defensive techniques can target specific attacks (e.g. antivirus signature-based techniques) or generic attacks (e.g. anomaly-based techniques). The latter are generally more effective against unknown attacks and less effective against known attacks. Cybersecurity typically includes traffic or event monitoring, attack detection and prevention, tracking, incident management and emergency response, and information sharing, i.e. reporting about incidents in cyberspace. Since unprotected data appears to be easier to monitor and track, in some circles there may be a belief that it is possible to achieve cybersecurity without data privacy.

Yet, we think that this is a misconception, since unprotected data gives rise to cyber attacks by less sophisticated attackers. Instead of concentrating on attacks and defences only, the position of the PST AL is to proactively address security and privacy in cyberspace. This can be achieved by promoting the adoption and deployment of innovative techniques and technologies that will render the systems and components used more reliable and trustworthy, in addition to the classical methods of building customer trust on the basis of reputation and best practices only.

Priorities
Consequently, the selected PST AL priority areas in the Strategic Innovation Agenda (SIA) 2014-2016 are: privacy-aware e-ID federation and strong authentication; protection of data privacy in online and mobile applications, services and communications; and mobile cybersecurity addressing the protection of computing devices against malicious software and intrusions. The PST AL is fostering innovative solutions in all three interconnected areas, and the expected success predominantly depends on the business orientation of the involved partners, as well as on their quality, dedication and determination.

The solutions for federated e-ID management and access control (of persons, things, services, legal entities etc.) will boost new ICT products and services, both nationally and internationally, but with the existing weak (password-based) authentication methods and without appropriate privacy-aware mechanisms, this would likely decrease security (due to federated passwords and single sign-on) and further downgrade privacy (due to profile linking and online profiling of identified citizens rather than pseudonymous users only). The current practice regarding data privacy is unsatisfactory and far from the minimality principle, especially for ordinary people and with respect to sophisticated adversaries. Due to the ever increasing usage of smart mobile devices containing both personal data and sensitive business-related data, and rapidly multiplying and evolving malicious or potentially dangerous apps for mobile devices, the existing solutions used in practice are partial and fragmented and do not appear to be sufficiently effective.

A paradigm promoted by the PST AL is to support data privacy by practical cryptographic techniques, including privacy-preserving data mining and profiling, secure multiparty computation, homomorphic encryption, secret sharing, anonymisation, anonymity protocols, anonymous credentials, attribute-based encryption and searchable encryption. Practical implementation of new solutions in the three priority areas requires developing appropriate security platforms and mechanisms in both software and hardware.

Synergies with the Horizon 2020 research and innovation projects are desirable and very likely and would certainly be beneficial. However, we feel that the current Horizon 2020 programme for 2014-2015 should have been even more adapted to the PST AL by anchoring data privacy and trust in digital technology on technical development, rather than societal aspects, and by explicitly emphasising the software and hardware security topics.