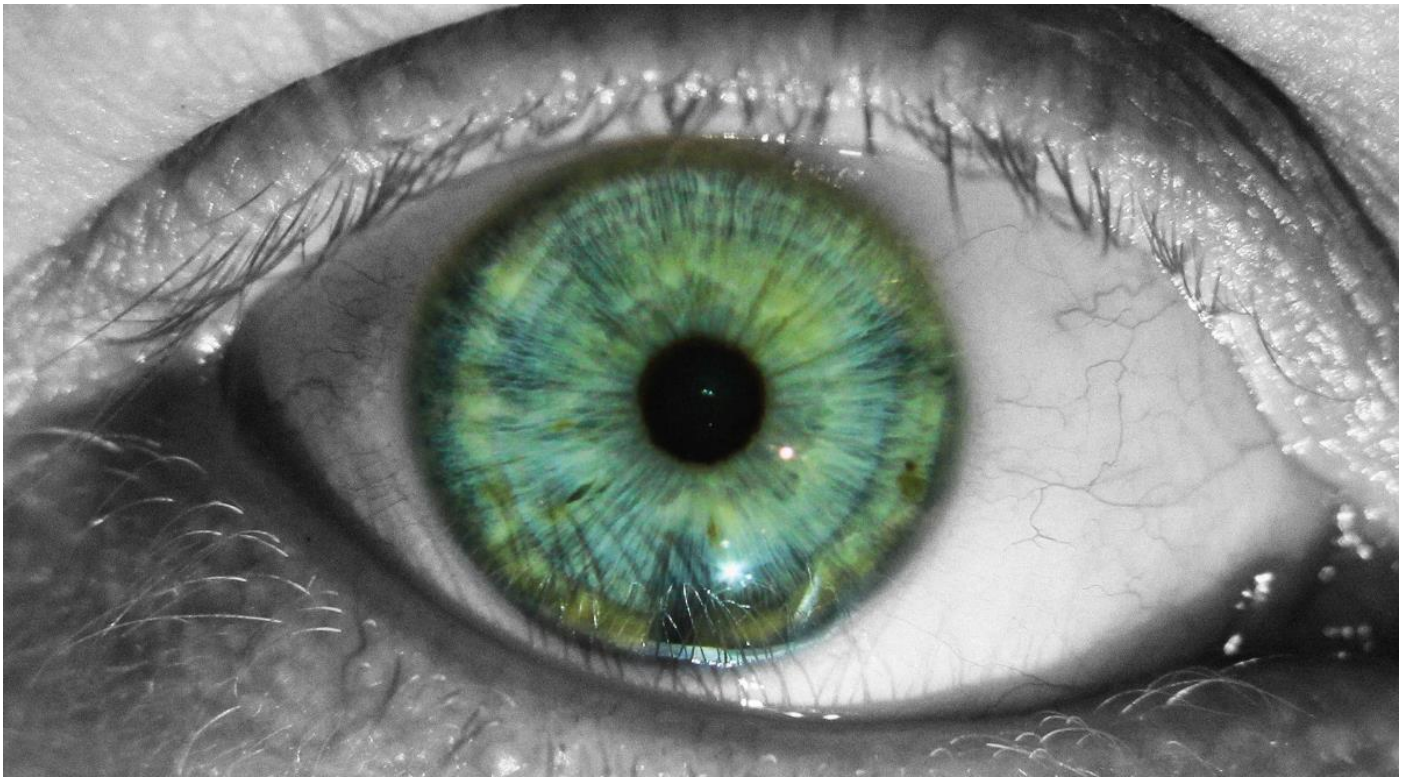

Privacy – an endangered species in a digital world

By Johann Čas

Published on **EuroScientist**: www.euroscientist.com

EU Citizens have been far too passive in responding to their exposure to digital surveillance

Privacy is often presented as something that we need to sacrifice or to trade off against certain benefits such as access to communities via online networks or even banking or telecommunication services. The trade-off approach is particular important when security comes into play. Surveillance technologies are often taken as a tantamount to security technologies. And privacy is presented as the price we need to pay for more security. This trade-off thinking is largely informing public debate and still dominating decision making on security policies. However, the growing surveillance—despite being exposed in recent years—has triggered feelings of helplessness among citizens against infringements of their privacy. This brings a lot of question on how our society handles surveillance and security. And now it is time for citizens to express what kind of trade-offs between privacy and security are acceptable.

Invasive technology

Technology is eliminating many barriers that used to protect our personal data and our privacy. Visions of ubiquitous computing are increasingly becoming a reality; what we buy, what we read, what we search, what we communicate with whom, where we move, almost all activities of our daily life leave digital traces.

Thus, escaping from pervasive surveillance, insofar as possible at all, largely implies a deliberate exclusion from full participation in professional and private life. Only a few spheres are left, like reading our brains. And even those are already in the focus of emerging technologies. However, there is no need for such dystopia to become a reality. The

EuroScience | 1, Quai Lezay-Marnésia | F-67000 Strasbourg | France
Tel +33 3 8824 1150 | Fax +33 3 8824 7556 | office@euroscience.org | **www.euroscience.org**

analysis of existing data is largely sufficient to find out—or at least guessing—how someone feels and thinks or what their political attitudes or sexual preferences may be.

The virtually unlimited possibilities to generate, collect, store, combine and process data do however by no means imply that these possibilities must or should be exploited without limits. On the contrary, the more data are accumulated and the more capabilities to use and abuse them exist. Then, the more important effective data protection regulations become. In addition, the easier infringements of privacy turn out to be, the more crucial its defence becomes.

Privacy rights

Data could be regarded as the crude oil of the digital age, fuelling the engines of future economic growth. Such raw material must therefore be used with caution to avoid data pollution. Once in the wild, poisonous chemicals or greenhouse gases are difficult to remove and produce long-term impairments to the natural environment. The same holds for data. It may not only infringe personal privacy but pollute the social environment and erode pillars of democratic systems—assuming that privacy is a prerequisite for further fundamental rights.

And our privacy has had a difficult few years. In 2013, Edward Snowden exposed the mass US and UK surveillance programmes. The documents provide an impressive body of evidence that the technical capabilities of surveillance technologies are exploited without virtually any restriction. Of equal concern, is the lack of an adequate public reaction and protest from European politicians to these revelations. Even the vigorous protest by Angela Merkel against such US surveillance practices, after the initial shock of the discovery, did not put an end to mass surveillance of the general public.

The idea for an investigation about the perception by EU citizens of surveillance and its implication for the trade-off between privacy and security was already born before these disclosures. This topic has been the object of an EU-funded research project, called, SurPRISE, completed in January 2015. It adopted a participatory approach involving about 2,000 European citizens via what were dubbed Citizen Summits and Citizen Meetings. Participants were consulted on their views on what trade-offs would be acceptable to balance security versus privacy, as they evaluate different security technologies and measures.

Citizens perspectives

The findings confirm the scepticism against the trade-off approach in general and, in particular, as a suitable guideline for decision-making related to security policy.

The participants predominantly requested strict limitations and regulations with regard to the use of surveillance technologies. Incidentally, these demands match the recommendations developed by high level expert groups; namely that of the Ethics of Security and Surveillance Technologies report of the European Group on Ethics in Science and New Technologies (EGE) and that of the The Right to Privacy in the Digital Age report of the Office of the United Nations High Commissioner for Human Rights. The recommendations are also in accordance with core objectives of the upcoming regulation and directive on personal data protection .

Participating citizens also believe that the protection of privacy and personal data by updated regulations should be strictly enforced. They demanded that authorities responsible for privacy protection enforcement should allocated sufficient resources. What is more they saw the use of surveillance-orientated security technologies (SOSTs) as only suitable when targeted and accompanied by adequate and strict safeguards such as mandatory comprehensive technology assessments including privacy impact assessments. They also consider its use justified and justifiable on a case-by-case basis, but did not accept blanket mass surveillance.

Trust into institutions conducting surveillance was regarded as a key factor for its acceptability. The participants raised the need to mainly allow surveillance activities by public authorities, whereas restrictions and limitations should be in place to permit surveillance by private sector actors. This also means that people consulted expected enforced and increased accountability, liability and transparency as measures to create trust and to prevent abuse.

EuroScience | 1, Quai Lezay-Marnésia | F-67000 Strasbourg | France
Tel +33 3 8824 1150 | Fax +33 3 8824 7556 | office@euroscience.org | www.euroscience.org

To top it all up, citizens wanted to be actively informed about how they can protect their privacy with respect to new information technologies, and in particular, to SOSTs.

Tackling inequalities

Last but not least, the participants requested a more comprehensive, holistic and long-term approach to tackling security issues. They were concerned that the authorities ought to put a stronger focus on the root causes of insecurity. This means tackling the enormous economic and social injustices resulting from the persistent economic crisis in Europe.

They clearly saw that SOSTs should by no means replace--but only be used in combination with--non-technological measures and social strategies addressing the social and economic causes of insecurity. People consulted considered a stable socio-economic environment as being an essential precautionary measure. And this, not only against minor crimes but also against increasing violent radicalisation at an individual as well as political level.

It emerges from this research that listening to the voice of citizens would therefore reduce the need for surveillance. In addition, it would also lessen resulting risks for privacy breach and related fundamental rights attacks. In turn, they saw such balance approach as a means of fostering democratic and societal development in line with European values.

Johann Čas

Johann is an economist, researcher specialised in the societal impacts of information and communication technologies, at the Institute of Technology Assessment, Austrian Academy of Sciences, Vienna. His current work focuses on data protection and privacy in the information society, privacy-enhancing technologies and their deployment within ambient intelligence, security technologies and health related applications. He was the coordinatory of the SurPRISE research project.

Photo credit: Tom Blackwell

EuroScience | 1, Quai Lezay-Marnésia | F-67000 Strasbourg | France
Tel +33 3 8824 1150 | Fax +33 3 8824 7556 | office@euroscience.org | www.euroscience.org