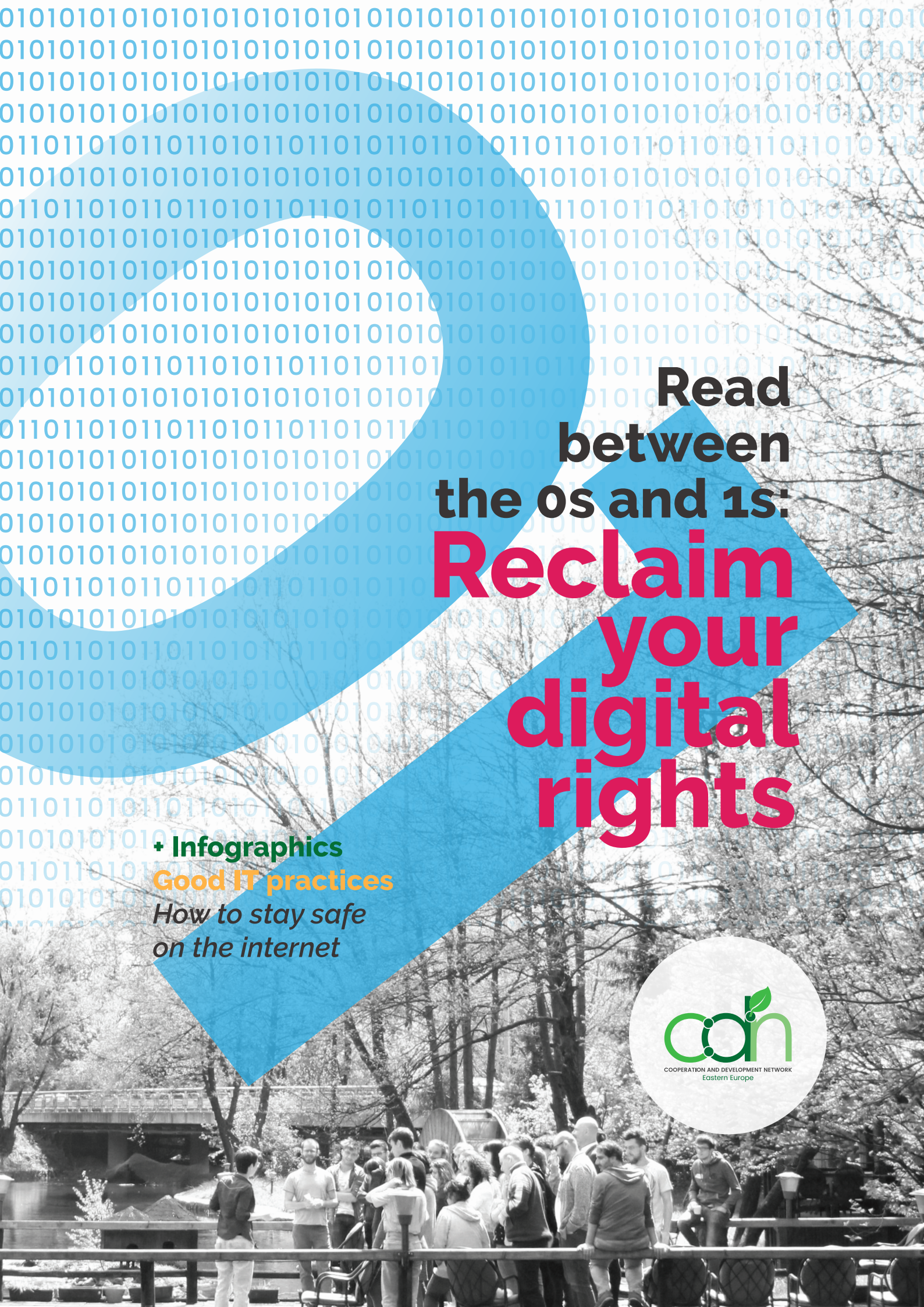
Read between the 0s and 1s:

Reclaim your digital rights

+ Infographics

Good IT practices

How to stay safe on the internet



COOPERATION AND DEVELOPMENT NETWORK
Eastern Europe

TABLE OF CONTENTS

COOPERATION AND DEVELOPMENT NETWORK
Eastern Europe

PUBLISHED BY
Cooperation and Development Network Eastern Europe
Rue Wiertz 31,
Brussels, Belgium/
Dr Dragoslava Popovica 22,
Belgrade, Serbia

LAYOUT
Design & typesetting:
Milan Nikolovski
Logo: Milan Nikolovski

Authors

Articles:
Bojan Stojkovski, Macedonia
Gergely S. Császár, Hungary
Žiga Rus, Slovenia
Maja Živković, Montenegro

Case studies:
Lea Caillère Falgueyrac, France
Michael Oghia, Serbia/USA

Infographics design:
Masha Dzneladze, Czech Republic;
Nikoleta Petkovic, Serbia

SORM authors:
Weronika, Meri, Cansu, Yulia, Lera, Maja

Cartoon authors:
Arpine, Dean, Lera, Vital, Yulia, Sara, Weronika

PICTURES
Cover & Backcover:
Djalel Boukerdenna

Page 3: Djalel Boukerdenna
Page 4-5: Daniel Friesenecker
Page 8-9: Andrew Martin
Page 10-11: Olya /Voloshka
Page 12-13: Amy Cheung
Page 15: Matthew Henry
Page 16-17: Werner Moser

DISCLAIMER
The content of the publication reflects opinions of individual writers, not necessarily those of CDN or its partners.

PARTNERS

green forum
GREEN EUROPEAN FOUNDATION
The Greens | EFA in the European Parliament
Internet Society
Internet Society Serbia Belgrade Chapter
one world platform
EYF european youth foundation
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

SUPPORTED BY
European Youth Foundation

INTRODUCTION

Read between the 0s and 1s: Reclaim your digital rights

Dear reader,

Do you like playing games? Me too! Now with all these smart devices and the Internet, it's easier than ever – well, at least easier than exchanging CDs of suspicious origin and trying to "crack" it for 30 minutes on your PC in order to play a low-resolution version of Need for Speed. Recently, I installed one of these guess-the-word games on my phone to play with a couple of friends. You hold the phone on your forehead, everyone but you can see what's written on the screen, the others give you clues, you guess, everyone laughs – it's fun; because games should be fun.

It took me two minutes to install it. So simple! It's funny to remember how I was taught program installation when I got my first computer 15 years ago: "Insert the floppy disk, open the file, and just click: next, next, next, next, finish! Simple as that." Who knows how many programs I installed this way without realizing that I can damage my computer if I don't read what I actually gave the program permission to do.

Now I know how the software is installed on a computer, I know 0s and 1s, and even some basics of programming. But I have to admit: sometimes I don't read the Terms & Conditions. Why? It's the same story every time: I start reading, but then I don't understand what all of it means, and second, I'll install this app anyway, so why bother? And then the game begins. For the sake of efficiency, as friends can't wait that long for me to read all of these conditions, I gave the app access to a couple of things: my identity, location, photos/media/files, camera, microphone and Wi-Fi connection information). Scroll, scroll, scroll… accept!

But wait a minute; why does this app need access to all of this information just to show a couple of words on the screen? It won't record us while playing – it would never do that, right? Wrong. I'm sitting in my room with friends, and I don't feel like sharing with the rest of the world what we do, what we laugh about, the issues we're passionately discussing. But the app doesn't care; it only does its job, what it was programmed to do. In fact, I consciously gave it the right to record me, so how can I complain?

My smartphone is the first thing I see when I wake up, and the last thing I touch before I fall asleep. It's an extension of myself; it's never more than a few meters away from me. It makes my life easier. So, it disturbs me when I can't trust this device. This smartphone, as well as any other tablet, PC, or recently growing network of smart things (such as a fridge or a toothbrush) are always connected to the Internet – along with almost 20 billion more devices. Our personal data is connected to our accounts, which we synchronise with all of our devices. Then we browse the Internet by sending our information from one server and service to another – across the world, faster than a blink of an eye. So, if one simple app can record what we do, imagine how much information Google and Facebook have about us. Creepy, right?

Where does our (meta)data go? Who can access it? Do we have a right to not share our information? And who should protect us? Should we be more concerned about what companies or governments do with our data? What level of awareness or kinds of reforms did Edward Snowden's revelations bring about? What excuses do our government use for mass surveillance? Which international regulations are there to protect us, and given the amount of distributed denial-of-service (DDoS) and ransomware attacks, can they even do so? Is technology developed in a neutral fashion, or do dubious human intentions shape it? Who runs the Internet? And how on earth do we protect ourselves?

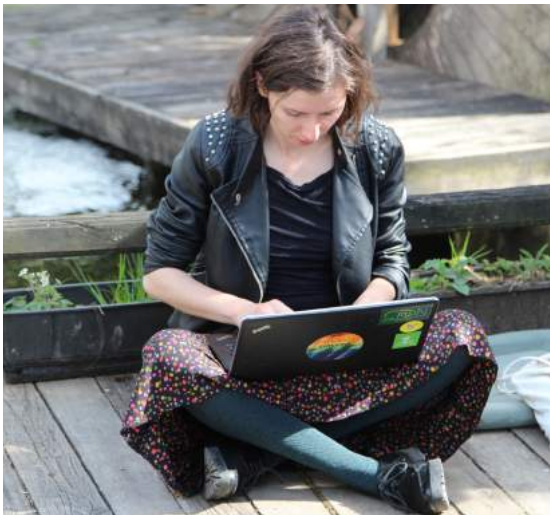
A group of young Greens from Eastern Europe wanted to find answers to these questions, so we organised a week-long seminar in Sarajevo, Bosnia and Herzegovina, to explore these questions, understand the security discourse, and how restrictions to online freedoms pose a threat to democracy, youth participation, and human rights. We invited 40 of our peers – young Greens and digital rights enthusiasts – and paired them with some great people from the Internet governance community, digital activists, hacker communities, and the European Green political family to share their experience as well as find ways to support young people in protecting their rights online.

Out of solidarity with our peers, fellow activists, and everyone who is concerned about their online safety, we created this publication to share different approaches regarding the issue, and to contribute to creating a more just world. In the following pages, you'll read about Internet and the media, digital rights as human rights, Internet profiling, as well as a sci-fi story that will draw you into a Black Mirror-like world. And the case studies we prepared won't leave you indifferent for sure. Don't worry, though, we included a couple of infographics to help you easily incorporate some online safety tips, and navigate the myriad privacy and cybersecurity tools available.

This is just the beginning of our digital security fight. We invite you to read and share this publication, and join the struggle for a greener and safer world for everyone.

Stay safe online!

Katarina Pavlović
CDN Office Coordinator, and preparatory team member of the "Digitised Security" seminar



INTERNET AND JOURNALISM

Professional information vs. "fake news"

by Bojan Stojkovski

In an era when online journalism is the norm and this type of media presents practically unfair competition for more traditional media outlets, quality and verifiable information remains the main pillar of journalism, and hence of democratic society.

We discussed this topic with Internet expect Frederick Donck, the director of the Internet Society's (ISOC) European bureau. Donck was one of the experts who delivered a workshop during the "Digitised security: How to read the surveillance discourse and fight it!" youth cybersecurity and digital rights seminar in Sarajevo in April, organized by the Cooperation and Development Network Eastern Europe (CDN). The event addressed the dangers that exist in the cyberspace as well as the role of online media in modern society.

According to Donck, although many thought that the growth of the Internet will also be a signal for the end of traditional journalism, the effect in modern times may just be the opposite because the large quantity of information has led to more filtering of the content we consume.

The effect in modern times may just be the opposite because the large quantity of information has led to more filtering of the content we consume.

"At the beginning of the Internet, as the network grew bigger and bigger, everyone predicted the end of the traditional media – in this case the newspapers – because through the Internet, everyone could become a journalist," Donck said. "Of course, newspapers need to compete with other online

media: they must have big audiences, as well as advertisements. But what I now see is that people want professional information, so I believe the right journalists and media who can offer it will survive. Certainly they will have to offer better quality news, analysis, and reliable sources, so I believe that the future of the Internet does not mean the end of classical journalism and traditional media. People say that, today, they trust more sources, but it's important to know that reporting must be done professionally and with quality."

Media reputation is based on quality and verified information

The good reputation of the media is always based on quality and verified information, something that is currently rare and must be constantly highlighted, he added.

"The trend we are seeing now is that people are increasingly trusting media with a good reputation and someone who can confirm their information with real facts. It is perhaps an upgraded form of journalism, where journalists present certain information and thoughts, but they all reinforce it with facts and relevance because now there is a great fear from the so-called 'fake news.' Perhaps the Internet brings new professionalism to journalism, which is really good," Donck said.

Raising awareness about cyber threats – a key role for the media

The media also plays a key role in raising awareness of the various ways in which data and information can be misused, the Brussels-based expert added. "The media is part of the information system, and their task is to warn people of the dangers that exist on the Internet," Donck said. "Perhaps the main reason for this is that people no longer trust the Internet, they think someone is always watching or following them online, or they are concerned about what happens to their personal information. The real debate is that people using the Internet should be able to manage the data they share, at any moment they need to know where and for what purpose their data is being used, how long some companies or institutions keep that information, etc."

QUIZ

Test your knowledge!

Case 1: Britain's version of the NSA taps fiber optic cables around the world

The British spy agency, the Government Communications Headquarters (GCHQ), taps fiber optic cables all over the world to intercept data flowing through the global Internet, we learned. The GCHQ works closely with the NSA, sharing data and intelligence in a program that's codenamed Tempora.
Tempora is one of the key NSA/GCHQ programs, allowing the spy agencies to collect vasts troves of data, but for some reason, it has sometimes been overlooked. After a couple of months from the Tempora revelation, a German newspaper revealed the names of the companies that collaborate with the GCHQ in the Tempora program: Verizon Business, British Telecommunications, Vodafone Cable, Global Crossing, Level 3, Viatel and Interoute.

Case 2: The Beirut, Lebanon-based Gulf Centre for Human Rights (GC4HR) recently began working with local activists in Kuwait to challenge a recent decision by a major school in Kuwait City.

Many parents have contacted the school's administration about allegations of terrorist propaganda being spread around Kuwaiti schools. Even though the school authorities believe the fears are sensational and unfounded, they see it as a way to further monitor the students and increase security. As such, they want to expand their video surveillance capabilities and install facial recognition technology. The activists, however, are concerned about the student's privacy.

The GC4HR brought the case before the Kuwaiti supreme court, and the court agreed that facial recognition would not be appropriate for schools. However, they ruled that gesture recognition is permissible.
The GC4HR brought the case before a Kuwaiti court, and the court agreed that facial recognition would not be appropriate for schools. However, they ruled that gesture recognition is permissible. Seeing that gesture recognition would likely still violate the student's right to privacy, the GC4HR decided to take the case in front of the Kuwaiti supreme court

Case 3: Belarus uses telecoms firms to stifle dissent

In Belarus, the KGB and other security services have free, non-stop, remote access to both real-time communication and stored data in phone and internet networks.

Telecoms companies, including ones owned by Telekom Austria Group and Turkcell, allow this to happen by granting the government nearly unlimited access to their customers' communications and data. Operating in Belarus requires giving authorities remote-control access to all their users' phone and internet communications.

TIME

Guess which case is fake!

Case 4: Blue Coat and the Syrian Regime

A U.S. company that makes Internet-blocking gear acknowledges that Syria has been using at least 13 of its devices to censor Web activity there.

This was revealed in 2011 by the Telecomix-Collective, a well-established hacker group that helped maintain connections to Egypt and other countries when governments tried to shut down access during the Arab Spring.

The logs analysis suggests the Blue Coat proxy was used to intercept and analyse encrypted traffic (https). All the requests using the 443 port (dedicated to https traffic) and routed to some of the most visited websites in Syria include more information than they should.

Case 6: 93 days of Internet blackout in west Cameroon

In the night of January 17-18 a government-ordered blackout began that lead to 3 months without Internet for the 2 English speaking regions of the country.

The government temporarily cut all internet traffic nationwide, but then restored it, except for the two restive Anglophone provinces. Rather than enforce a nationwide cutoff once the point was made to the telcos, the government employed third party software it had purchased to carry out selective provincial blackouts.
MTN, the largest mobile operator in Cameroon with 57% market share, was one of the companies forced to suspend service, and was also asked to provide additional information on its customers by the Cameroonian government.

Case 5: Government hacking of nutritional activists in Mexico with Israeli spyware

Last summer, in Mexico vocal proponents of the first soda tax and activist battling childhood obesity in the country started received a series of disturbing text messages from unknown numbers. Some said their daughters have been in a serious accident. Another claimed to be from a friend whose father had died — with a link to funeral details.

The links sent to the men were laced with an invasive form of spyware developed by NSO Group, an Israeli cyberarms dealer that sells its digital spy tools exclusively to governments and that has contracts with multiple agencies inside Mexico

Solution: 2nd case

HOW I was almost SCAMMED based on INTERNET profiling

by Gergely S. Császár

Frankly, I believe I do not do enough to protect my privacy online. Sure, you hear a lot about how the lack of privacy affects us: how mega corporations are selling your metadata and online social activity to advertising companies, and how your every action is being surveilled by government agencies based on the argument that it is for the "greater good," thus it is vital for national security. Regardless, I was one of those who, after hearing about the Snowden revelations, went around my own circles, restlessly spreading the word about just how large the scale of this whole security apparatus is. At the end of the day, however, I continued to sit down in front of my computer, open Gmail or any other Google product, shrug my shoulders, and think: "For the convenience they provide, I am willing to sacrifice some of my privacy. As long as I am not doing anything illegal, I have little to worry about, right?"

I could have paid a hefty price for my ignorance. You see, I consider myself fairly active when it comes to politics – the number of international conferences I have attended in the past year that are closely related to human rights and Green political issues are double digit, which given that visibility is an important aspect of my organisation, I was happy to share with the rest of the world. Yet, some in the world were happy to abuse this information.

Do you get scam e-mails? You know, the sort where a Nigerian prince has recently passed away, and due to the mysterious and highly fortuitous circumstances of Fortuna you are the sole inheritor? Or where you were just awarded an international prize for playing a lottery you have never heard of? Well, scammers develop alongside technology, and I have found that they have more convoluted and convincing ways to empty one's pockets than I had previously suspected.

So, on a sunny Tuesday afternoon, an email landed in my inbox. A conference invitation in the title, my interest started tingling with fascination, as my hand moved to the mail and my eyes started scanning the contents. "The Cooperation for Sustainable Development invites you to a conference on LGBTQI rights in developing countries," read the first line. Sure, the NGO sounds generic enough, but the list of speakers was extensive, the agenda seemed convincing, and the topic interesting enough to draw my attention. The location, however, was a bit trickier: Austin, Texas. I scratched my head for a minute; how it would be possible on a very limited budget to fly to the United States from Hungary and back? But the more I read, I found the paragraphs I needed to comfort me, for upon further request, they wrote they could provide some financial support pending they met the conditions listed in the email.

My initial enthusiasm was followed by scepticism. The first suspicion arose from the fact that the invitation was lacking an official signature, although that is not uncommon in small NGO circles. The mail was signed by the organisation's secretary-general. A quick search found her LinkedIn profile, which, although lacking a picture, did state her employer as Cooperation for Sustainable Development. The organisation even had a working website, with clickable menu items, contact details, tax number, and a picture of the team during a workshop. The photo was rather low quality, so I thought about running it through Google's image search hoping to find out more about the organisers and the board apart from the very generic statement found on their website about their vision. This is when the interesting revelations began.

First, it turned out that the picture was taken years earlier, and depicts a U.S. city planning commission from San Francisco, California. Second, upon further research, I found a person by the same name as their secretary-general working for UNESCO on a completely unrelated topic. And third, the website disappeared without a trace two days later.

People can access our contacts, and more worryingly, our interests and what possibilities we might jump on if we are caught off guard.

Unfortunately, I do not know what would have happened had I contacted them about the details of my travel arrangements. I do not know how they got ahold of my email address, and how did they know my specific interests and my habit of attending international conferences related to the topics they advertised. Honestly, I do not even know who they were. What I do know, however, is that our profiles are out there. People can access our contacts, and more worryingly, our interests and what possibilities we might jump on if we are caught off guard. In my case, they even went to the lengths of investing both energy and time into setting up fake websites to convince me that they are genuine and working for the same cause that I work for.

Around a month later, the scam was back again: another email, from another generic organisation, with an invitation to a conference in Texas.

The scariest in all of this is that I have always regarded myself as a more cautious type when it comes to my digital security. I never shared passwords, never shared contact information when considered unnecessary, never subscribed to obvious scams, and always remained cautious and vigilant about my online presence. And yet, it was not enough. This is why events like the Cooperation and Development Network of Eastern Europe' (CDN) Digitised Security youth seminar are vital, especially for activists. Learning about the bare minimums of what you can do to remain safe and secure online and hide your activity from unwanted eyes is a must, and providing people the information on how to do it is not a possibility; it is an obligation.

THE MORNING

Writer: Žiga Rus
edited by: Michael J. Oghia

A cheerful alarm sounds at exactly 09:30:00. Some grunts are recorded by the time keeping mechanism, some movement detected by the nocturnal rejuvenation pad. All of a sudden, a change of pressure is registered on the pad, slightly toward the middle – sitting confirmed. The interior monitoring system detects a slight irregularity in the air currents; a small quantity of air is being deeply inhaled at 79 psi and exhaled at 74 psi.

Pad pressure again changing, and now pressure being detected by the floor; feet identified, the pressure recognized as steps. Steps moving from the nocturnal activities quarter toward the hygiene station. The tempo of walking is a mere 68 percent of the statistical average, the trajectory deviating a bit from the standard, not totally straight – this data being automatically contrasted against the data from previous night, including an analysis of the number of beverages drunk, the quantity of alcohol in the beverages, current electrolyte levels, and other metrics.

With the mirror activated, a face is recognized. Facial evaluation initialize: the skin under the eyes more dark and wrinkled than average; skin tone a little paler than usual. Overall well-being decreased. Zoom in: some eye redness is also detected. With morning inspection completed, one command for a café latte to individual liking is processed.

Steps moving toward the front of the human waste disposal apparatus. The bowl detects a new liquid input: the amount of the liquid higher than standard, but falling perfectly into the pattern of every sixth morning of the week. Steps away and the apparatus purges its contents, the water consumption strictly within the limits of the water consumption law.

Steps moving to the organic energy preparation area, now in front of the organic energy cryostorage unit. Upon activation, it proclaims its morning greeting. Eye scan initiated: analysis indicates essential nutrients depleted; high levels of oxidation and free radicals detected; rehydration necessary. The unit locks; "Your body requires conditioning for nominal functioning," a robotic voice states. "Commence physical conditioning program." Some holographic instructions are provided; the unit counts the sit-ups, and then tenderly suggests push-ups and squats. Finally content and registering a return to more nominal metabolic processing, the unit unlocks.

The organic energy preparation device analyzes the items inside to create a meal optimized for the subject's current condition. It takes Grupo Bimpo™ product no. 39586929109949493 and combines it with some HealthyJam™ product no. 132249594939393, Dole Company™ product no. 5869219109294950291, and United Cereals™ product no. 52920502192096979 to create the exact balance of vitamins, minerals, amino acids, omega-3 fatty acids, and electrolytes needed to return the body back to its default homeostatic state. An optimized café latte concludes the energy infusion process.

After the morning energy infusion, an information-recording device is picked up. With the ink simulator, some lines are drawn on the e-paper and recognized first as letters, then as words and sentences. Some thoughts about yesterday. Some resolutions about the future input of potentially intoxicating liquids. Some regrets about missed opportunities for new acquaintances (heart rate increases, blood pressure rises – both detected by the SmartFabric™ bodily functions recognizer). Some individuality is enjoyed, all stored conveniently. At the same time, the InstaWrite™ app is improving the content and style of the writing in accordance with the writing filter of choice: Joyceian, Proustian, Kafkaesque, Hemingwayesque. At the moment, the Proustian mode is activated: short sentences are merged into longer and more complex ones, and some poetic thoughts about memory and biscuits are seamlessly incorporated in the original text.

The pressure on the body support unit is not complying with the Healthy Sitting Standards, so the unit issues a warning that a better posture is possible. When pressure adjusts, the unit emits a commendatory sound. By that time, the SmartBrick™ system is already discreetly alternating between yellow and green, alerting the subject that the dental hygiene routine must commence. Steps are moving from the organic energy preparation area to the hygiene station again. The

dental hygiene facilitation device is being picked up, its moisture receptors detecting the mouth's environment. The force on the bristles of the device mirrors the form of the subject's teeth: the filling on the second molar, the right wisdom tooth bulging under the gums. The device plays an encouraging song until the mouth environment is processed as recommended by World Mouth Hygiene Resolution no. 34,524.

After the lonely morning period, the Network is finally activated. Holograms fly around the subject and are moved through the space by the subject's hands: new stories from friends, photos from breakfast, and TubeMe™ videos and information articles shared. Some responses are produced by the subject; mostly likes but even some loves, the later being consistently given to the same few contacts. Some articles are shared, as well as a memory from three years ago and a friendship anniversary. An increasing heart rate and a change in breathing is detected again, connected with information that is being viewed at the moment, and analyzed: pictures of travellers, of nice evenings with friends, of first novels being published. The bodily changes, emotional response no. 654,435.234 is recorded as "standard Network jealousy," and stored in the emotional history file.

Typing on the virtual keyboard is fast and forceful, betraying an impulsive personality. The history of the subject's consumer behavior confirms the theory: commercial triggers are often successful, and the time between the trigger and the actual purchase usually quite swift. Today is no exception; **after hastily reading an article on the Network – something about the perils of digital profiling – an algorithm quickly offers the subject an e-book on the matter, and in the next 50 seconds, the offer is accepted.** The book is promptly downloaded into a folder of the information-recording device where, admittedly, it will probably wait for quite some time (the average time spent reading: 3.7 hours per week, with approximately 27% of the books actually being finished).

Finally, a special event invitation on the Network grabs the subject's attention. The city museum is offering a new and intriguing virtual tour to "the time of our grandparents." "Visit the 1980s!" announces the invitation:

"A time with no connectedness at all. What a curious period this must have been. Nothing to entertain yourself with except books and television with the most limited number of channels; unmovable phones that allowed only for voice conversations – the most unenjoyable and clumsy way of communication. And if you left your home, how many unnecessary complications! No talking with anyone unless they are in the same physical space; big paper maps that you had to actually carry with yourself if you didn't want to get lost; not to mention all the physical contraptions that one had to buy and carry home on their own."

Some bodily changes are again detected by the bodily functions recognizer: this time, with regard to the context, they are labeled as "cheerful + curiosity," and again stored in the emotional history file. Almost immediately, the purchase of the tour and the time of the delivery are selected. Soon, the museum drone will deliver the virtual reality headset and other necessary equipment at the subject's door. The bodily functions recognizer, however, detects some physiological signs of hesitation as well, and stores them as a hypothetical "fear of boredom." But there is really no reason for such apprehensions, as the tour only lasts for an hour, and a special code for the termination of the tour is given to all customers at the start. After all, the museum is there to entertain, not to torture its customers, and lawsuits must be avoided at any cost.

***

The Shepherd leaned in his old office chair – they don't make them like they used to – sipped some coffee that he made in an old coffeemaker – they don't make them like they used to either – and inserted a CD in his Discman. Since no new Discmans have been made for years, he found this one, a rarity, one Saturday on a flea market in a remote part of the city. Even flea markets are a rarity these days, he thought.

Before him, an immense interwoven web of lines and

dots was displayed on a gigantic screen. For most of the people, understanding it was clearly hopeless – but not for him. Of course, it took him a few years of daily practice, in spite of his high score on the perception ability test. But after couple of years, he could almost see the people behind the lines on the screen – where they are, what they are doing, how they are feeling about it.

In his more anxious moments, The Shepherd was mildly worried that, given the high abilities of the system itself, his job could one day be replaced by just another systemic function. A system that watched could as well be a system that decided itself, on the base of the principles that it received, to which subject special attention should be given. Even now, the system made the majority of the recommendations, and in most cases, The Shepherd obeyed them. But he could also sense that the government was not really happy with the idea of leaving it all to the system. They had this feeling – he assumed – that at the very last level, there should still be a person, a human being.

Which was actually a pretty humanist way of thinking, he thought, and took another sip from the cup.

And the government was a humanist one, really, if you think about it, and kind. They let people do any variety of things, read a variety of books and articles, discuss a whole range of topics, while also gently nudging them in the direction of a healthy, fulfilling life. Nudging, not violently pushing – that was their main strategy, and it worked formidably. Most of the people were totally content with being nudged, and the overall degree of happiness – as measured by the amount of data that suggested anxiety – was very high.

Of course, among the people many different opinions emerged – even ideas of alternative societies, alternative ways of living. But what the government came to realize was that if you leave the people relatively well fed and give them an impression of a steady progress, nothing much really happens. Almost all the contrarians stayed within the limits of non-threatening behavior: sharing articles and writing angry posts, but nonetheless still waking every day on their connected mattresses, doing their morning exercises in front of the fridge.

Still, there was a tiniest fraction of the society who tried to put their newfound principles into action – and threatened the social cohesion while doing so. In those cases, the government of course had to intervene as quickly as possible, and the steady influx of data has proved to be most helpful in doing so. The Shepherd had a slightly uncomfortable feeling when he thought of those people, of what might happen to them. But he knew that those feelings pass pretty quickly. Every society, he reasoned with himself, had some norms, and sanctioned those who threatened them. The world they were living in was without doubt as close to perfection as it was ever possible. It took humanity so much time to come to this extraordinary point in history. You can't really oppose something that's nearly perfect just because it is not perfection itself.

The Shepherd directed his gaze to a swarm of dots that has become just a little bit redder this morning. It was almost imperceptible if you were not a shepherd or a machine. Some of them have read some dubious-sounding articles; the others were interested in some dangerously sounding events. But it was alright; there was nothing criminal in these deeds. Most of them will get paler over the course of next days, and even if not, their red color would have to become much more intense before the government decided it was time for action. **The field of freedom was vast and most of the subjects never came to the border. To stroll a little bit in one way or another was all that this flock really needed, or at least most of them did.**

He listened to his body. Was the uncomfortable feeling gone? That was one luxury of being a shepherd – you were provided with some old-school clothes, not those ridiculous connected shirts and jumpers that take notice of any change in your pulse or blood pressure or breathing. It seemed to him that the moment of doubt was really over. The rest of the morning will probably pass without disturbances. He emptied his cup, reclining contently in his chair in a very unhealthy posture.

DIGITAL RIGHTS as HUMAN RIGHTS

by Maja Živković

Digital rights are human rights that allow individuals to access, use, and/or create public digital media or to access and use computers, other electronic devices, or communications networks; therefore, as stressed in the editorial *La Vita Catollica,* "What the law permits or prohibits offline must also be the case online." Yet, what is increasingly obvious in contemporary society is that we are not in the place that ensures that network use respects universal human rights, and by extension, digital rights.

In order to analyse digital rights violations on an individual level, in democratic societies (including societies that are called democratic, but it can be argued if they really are), let us consider some cases that have been presented to the European Court of Human Rights (The Court), in which The Court found that there had been (or no) violation of Article 8 of The European Convention on Human Rights (The Convention).

ARTICLE 8 OF THE CONVENTION

A *priori,* it needs to be said that the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of The Convention, and that "the domestic law must afford appropriate safeguards to prevent any such use of data as may be inconsistent with the guarantees of this Article." In the judgment *S. and Marper v. United Kingdom* from 2008, The Court found that "the need for safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data is used for police purposes, and that the domestic law should notably ensure that such data is relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored, as well as the domestic law must afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse."

..most countries do not have legislation - or (...) their legislation does not indicate with reasonable clarity - the scope and manner of exercise of the authorities' discretion in this area.

In the case L.H. v. Latvia, which considered the use of the applicant's health data, The Court recalled the importance of the protection of medical data to a person's enjoyment of the right to respect for private life, and therefore found that the applicant's right for her private life had been violated.

In the case *Perry v. United Kingdom,* which pertains to using the applicant's global positioning system (GPS) data; however, **The Court held that there was no violation of Article 8 of The Convention because it pursued the legitimate**

aims of protecting national security, public safety, and the rights of the victims, and of preventing crime. In this case, it is very important to say that GPS surveillance had been ordered after less intrusive methods of investigation had proved insufficient, had been carried out in a relatively short period (about three months), and had affected the applicant "only" when he was travelling in his accomplice's car. In the end, The Court found that the applicant's surveillance had been necessary.

SECRET SURVEILLANCE AS GUARDIAN OF SOCIETY?

Also, in the case *Klass and others v. Germany,* The Court noted that powers of secret surveillance of citizens are tolerable under The Convention only if so far as strictly necessary for safeguarding democratic institutions, as well as that the existence of some legislation granting powers of secret surveillance over the post and telephone was, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder of crime.

AUREA MEDIOCRITAS

Precedent *S. and Marper v. United Kingdom* should be considered again, related to what has already been said. This case concerned the indefinite retention in the database

of the applicant's fingerprints, cell samples, and DNA profiles after criminal proceedings against them had been terminated by an acquittal in one case and discontinued in another case. The essential message imparted by The Court was that any state claiming a pioneer role in the development of new technologies bore special responsibility for "striking the right balance." "**Balance**" in this case **refers to the relationship between privacy and security, which means that state must prove a fair balance between the competing public and private interests.**

The question raised is how to determine such a balance. As one might expect - the answer lacks a concrete, accurate response, which practically means that it depends on each specific case – that is, it depends on its facts and legal framework.

Nevertheless, it is possible to establish certain principles.

(MINIMUM) DEGREE OF PROTECTION

The case *Shimovolos v. Russia* concerned the registration of a human rights activist in the so-called "surveillance database," which collected information about his movements, by train or air, within Russia, and his arrest. The Court held that there had been a violation of Article 8 of The Convention, and found that the domestic law did not indicate with sufficient clarity the scope and manner of experience of the discretion conferred on the domestic authorities to collect and store information on individual's private lives in the database, and, in particular, it did not set out any indication of the minimum safeguards against abuse in a publically accessible manner.

Bearing in mind what has been said about The Court's practices, we can conclude that **most countries do not have legislation – or that their legislation does not indicate with reasonable clarity – the scope and manner of exercise of the authorities' discretion in this area. This is particularly imperative since it can – and in some concrete cases, does – lead, to the situations in which individuals do not enjoy the minimum degree of protection to which citizens are entitled under the rule of law in a democratic society.**

The case *Roman Zakharov v. Russia* concerned the system of secretly intercepting mobile telephone communications in Russia, and the applicant, an editor-in-chief of a publishing company, complained in particular that mobile network operators in Russia were required by law to install equipment enabling law-enforcement agencies to conduct operational-search activities. Therefore, without sufficient safeguards under Russian law, this permitted blanket interception of communications.

What is especially important in the ruling of The Court, which held that Article 8 of The Convention was violated, is finding that the Russian legal provisions governing interception of communications did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse, which was inherent in any system of secret surveillance. Moreover, such guarantees were absent even though the risk of abuse is particularly high in a system such as Russia's where the intelligence agencies and police have direct access, by technical means, to all mobile telephone communications.

ANTI-TERRORISM SURVEILLANCE VS. PRIVACY

Considering the current state of the security situation around the world, another important issue to consider is anti-terrorism surveillance, which was the main topic in the *Szabo and Vissy v. Hungary* case that concerned Hungarian legislation on secret anti-terrorism surveillance introduced in 2011. The applicants complained in particular that they could potentially be subjected to unjustified and disproportionately intrusive measures within the Hungarian legal framework on secret surveillance for national security purposes. The Court held that there had been a violation of Article 8 of The Convention, but accepted that it was a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies, including the mass monitoring of communications, in pre-empting impending incidents. The Court, however, was not convinced that the legislation in question provided sufficient safeguards to avoid abuse. The scope of the measures could include virtually anyone in Hungary, with new technologies enabling the government to easily intercept mass quantities of data concerning even people outside the original range of operation. Furthermore, the ordering of such measures was taking place entirely within the realm of the executive branch and without an assessment of whether interception of communications was strictly necessary and without any effective remedial measures, let alone judicial ones, being in place.

ADDRESSING DIGITAL RIGHTS

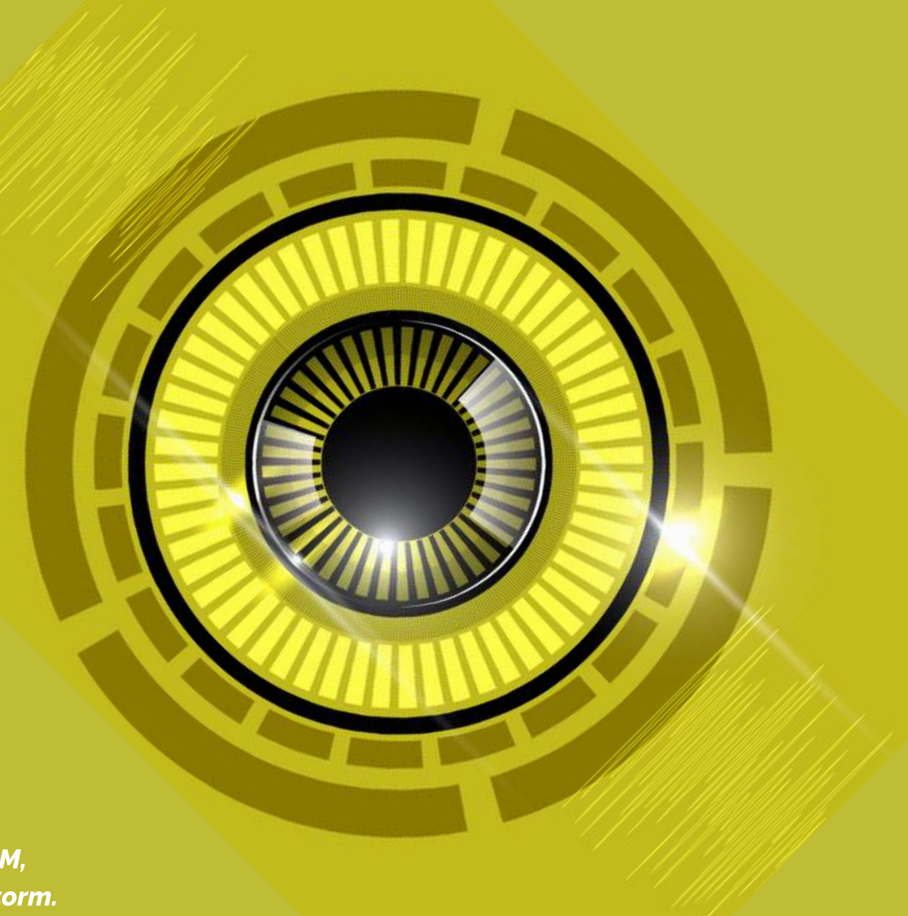
The conclusion that The Court should keep in mind is that it is the guardian of human rights on the European continent, so it is important to create a set of principals regarding digital rights, with the first and foremost of those regarding the right to privacy and family life. On the other hand, **it is clear that The Court needs to address digital rights in a new and improved level.** The rationale for this recommend was exemplified in the aforementioned case that The Court indirectly approved the mass monitoring – a gross violation of human rights.

Undoubtedly, The Court should divorce itself from politics and any other external factor that may affect basic, universal human rights, and should only have in mind the very essence of human life. Therefore, **there's a great need to raise awareness at every level, at every opportunity, so we can create a society aware of the importance of protecting individuals and their rights, and ensure this rationale becomes the norm rather than the exception.**

The Court, mostly, showed us that we can get the desired justice, but it is certain that that is not enough, not even close, waiting for years for someone to declare that someone had been right and that their rights were violated is discouraging and often almost pointless, too late, or at least not early enough.

In the end, *summa summarum*, preventive action is always best kind of action and, for sure, digital rights do matter.

“SORM: System for Operating Investigative Activities”



Today we will tell you the story of SORM,
Please be prepared for an information storm.
Belarus is the country where our story takes place,
But in many other countries, there is a similar case.

The name “SORM” stands for the System for Operating Investigative Activities;
We think it sounds like the issue involves many sensitivities.
This system enables surveillance of both the Internet and telephone communication.
We believe it’s crazy and it’s an enormous aberration!

The system was created in the Russian Federation,
And we all know about this country’s government’s reputation...
SORM has operated in Belarus from 2012,
Please listen to the story, and judge by yourself.

The main actors involved are special government services and police,
Other actors are the governments and ISPs.
It means that in Belarus people cannot sleep at peace.

The ISPs are obliged to provide 24-hour access for the special government services,
But probably they wouldn’t like to confess.
As we’ve mentioned other countries have similar systems,
The U.K. and Kyrgyzstan, for example,
So, the examples are ample.

When it comes to who is being watched,
There are really many targets that can make its purpose come to fruition.
Human rights activists, NGOs, citizens, the opposition,
As you can see, the SORM system would need much ammunition.

Even tourists and visitors can be controlled,
As you see, the system is pretty bold.

Now we would like to conclude:
We think that this system is rude!
If you want to know more,
Please ask us, therefore!

01011010 01110101 01011010 01110101 01011010 01110101 01011010 01110101 01011010 01110101 01011010 01110101
01110101 01011010 01110101 01011010 01110101 01011010 01110101 01011010 01011010 01110101 01011010 01110101
01011010 01110101 01011010 01110101 01011010 01110101 01011010 01110101 01011010 01110101 01011010 01110101
01110101 01011010 01110101 01011010 01110101 01011010 01110101 01011010 01011010 01110101 01011010 01110101
01011010 01110101 01011010 01110101 01011010 01110101 01011010 01110101 01011010 01110101 01011010 01110101
01110101 01011010 01110101 01011010 01110101 01011010 01110101 01011010 01011010 01110101 01011010 01110101
01011010 01110101 01011010 01110101 01011010 01110101 01011010 01110101 01011010 01110101 01011010 01110101
01110101 01011010 01110101 01011010 01110101 01011010 01110101 01011010 01011010 01110101 01011010 01110101
01011010 01110101 01011010 01110101 01011010 01110101 01011010 01110101 01011010 01110101 01011010 01110101

LOVE ACTUALLY 2.0

WATCH OUR NEW CARTOON!

CLICK HERE AND WATCH IT RIGHT NOW!

Our Youtube Channel:
Cooperation and Development Network Eastern Europe

INFOGRAPHICS

How to stay SAFE on the internet

GOOD IT PRACTICES:

How to stay safe on the Internet

SAFE BROWSING

WHY?

- Make sure that only you know what websites you visit
- Get around blocks and censorship
- Be anonymous
- Make yourself less vulnerable to criminals

There are various ways to make your everyday browsing safer and more free. Many of them are easy to use and free, too!

HOW?

- Use a VPN to get around censorship and improve privacy
- Install verified security plugins in your browser
- Make sure that the connection between you and the website is secure

EXAMPLES

- VPN: Zenmate (iOS), Psiphon pro (Android)
- Plugins: HTTPS Everywhere, uBlock Origin
- Use the Tor Browser for maximum security and anonymity

SOCIAL NETWORKS

WHY?

- Social networks are full of personal information
- Personal information should be under our control
- Stop companies from making money off you

The biggest social networks are run by companies who sell our data. However, there are some things you can do to make them a little less bad

HOW?

- Change who can see your posts
- Make as little of your profile visible to the public as possible
- Carefully look at and change the privacy settings

EXAMPLES

- You can use "view as" on Facebook to see what others can see
- Check what's under "Settings" -> "Privacy" on Facebook

PASSWORDS

WHY?

- Passwords are the keys to your online home, so keep your passwords safe
- If someone has your passwords, they can not only steal your information but pretend to be you

Passwords are crucial online, they are often the only thing that protects our identity and data

HOW?

- Use a password manager
- Don't use the same password for different websites
- Use good passwords, such as sentences
- Don't save passwords in a text file on your computer

EXAMPLES

- Password managers: KeePassX (Desktop), KeePassDroid (Android), MiniKeePass (iOS)
- A good passphraze: passphrasesarealwayshardertocrackthanshortwordsandnumbers

MOBILE & APPS

WHY?

- Almost all of us use smartphones everyday
- Personal information should remain personal
- Smartphone use can be made more private
- It's easy!

Our phones know much about us. Too much. We need to take back control and ensure that our personal information doesn't end up on the internet

HOW?

- Use open source apps
- Avoid apps by commercial companies
- Enable privacy settings
- Install via official app stores

EXAMPLES

- Signal (messaging application)
- OpenStreetMap
- F-Droid (Open Souprce app store)

ENCRYPTION

WHY?

Make sure that only those you authorise have access to your data
Stop others from listening in on or monitoring your communication
Make the lives of those who try to surveil us more difficult
Sleep well if your phone gets lost or stolen

Encryption helps secure both your communication with others and the personal data you keep on your devices

HOW?

- Use email encryption
- Encrypt your phone and your computer hard drive

EXAMPLES

- Android 6.0+ and iOS 4+ have encryption enabled by default
- In older Androids, enable it in the "Security" settings
- When setting up your computer, choose "encrypt hard drive"
- Use GPG for email communication

LINUX

WHY?

- Anti-capitalism
- It's a commons-based community project!
- It's very secure
- All versions are free

Linux is an operating system, like Windows or OSX, but made entirely from free software. It runs on everything from laptops to supercomputers

HOW?

- Download and install one of the many flavours of Linux
- And keep it updated to stay safe

EXAMPLES

- Linux Mint
- Ubuntu
- Majaro

www.cdnee.org

creative commons

These infographics were created by the participants of CDN's "Digitised security: How to read the surveillance discourse and fight it!" seminar, which took place in Bosnia and Herzegovina from 24th to 30th of April 2017. This seminar was supported by the European Youth Foundation of the Council of Europe, Green European Foundation, ISOC Serbia, and ISOC Europe with the local support of Youth Movement Revolt.

Internet Society Serbia Belgrade Chapter

Internet Society

REVOLT

GEF GREEN EUROPEAN FOUNDATION

EYF

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Preparatory team of Digitised security –
How to read the surveillance discourse and fight it! seminar:

Katarina Pavlovic
Julian Hauser
Mariam Khizanashvili
Michael Oghia
Léa Caillère Falgueyrac
Djalel Boukerdenna
Sopho Mchedlishvili
Antonela Ramljak

Click here and check more about digital rights!

This publication can be found at CDN website (www.cdnee.org)

COOPERATION AND DEVELOPMENT NETWORK
Eastern Europe