PLATO'S EU

Philosophical Learning Applied To Online Surroundings in EU

Draft and example for PRP2 workshop:

"Modern problems of privacy: What's my right to privacy in a digital era?"

Co-funded by the European Union

PLATO's EU

Version	Date	Comments
1	6.2.2023.	*First draft of the workshop developed for PRP2, offered to partnership for revision.*
2		
3		
4		

Document title:	*"Draft and example for 2nd Project Results Package 2 workshop"*
Date of issue:	*20.2.2022.*
Author(s):	*Filip Škifić*
E-mail address:	f.skifa123@gmail.com
Contributors to document:	
Quality reviewer (if any)	*n/a*
Number of pages:	*16*
Confidentiality status:	***For internal use of project partnership only***

The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

CONTENTS

The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

5th WORKSHOP:

"Modern problems of privacy:
What's my right to privacy in a digital era?"

The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

1. INTRODUCTION TO THE TOPIC

At the beginning of the workshop, the teacher/facilitator briefly describes the course of the workshop to his students. He explains to the students the goal of our workshop and that goal can be summarized by the answers on these questions:

- What is the right to privacy?
- What is digital privacy?
- Where is the line between private and public life?
- Did mankind had more privacy before digital revolution?
- Is it safe to share personal information to the whole world?
- Can your private information be misused?

What is the right to privacy?

The right to privacy encompasses the right to protect a person's intimacy, identity, name, gender, honor, dignity, appearance, feelings and sexual orientation. The right to privacy may be limited in the interests of others, under specific conditions, provided that the interference is not arbitrary or unlawful.

Digital privacy refers to the protection of an individual's information that is used or created while using the Internet on a computer or personal device. This concern is growing because browsing history and personal information online may be compromised.

The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

2. LESSON OVERVIEW

This workshop is a classical Socratic dialogue with stimulus in the digital world (recommended time: 45 minutes).

The main objectives of this workshop are:

- to show how changes in the digital landscape have impacted digital privacy

- to point out the importance of understanding the human right to privacy and its fragility in the contemporary world

- to encourage students to use critical thinking skills in a digital world and to understand the line between private and public life

Materials that should be used include:

- Mobile phones (it would be good if every student could use his or her mobile phone with an internet connection)

- Computer

- Projector

- Paper, pencil and other necessary educational materials.

Learning outcomes that will be attained through the workshop:

- understanding their digital identity and their role in a digital world
- understanding their human rights on privacy and freedom

The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

- understanding digital citizenship through access to reliable and credible information

3. LESSON BREAKDOWN – WORSKHOP ACTIVITIES

3.1. Part I. What is privacy?

The teacher starts the workshop by asking his students if they know what is privacy? There is no right answer but the point is to guide the students to make a difference between privacy and a public matter, regarding personal and public knowledge. After making that difference and defining privacy, teacher should ask them with whom they share their personal information. Students will probably answer that they share their personal life with family and friends and that's the time when the real stimulus starts. The teacher should tell their students to go on their social media profiles (facebook, Instagram, twitter etc.) and find information that is written there like name, date and place of birth, and their current location of living as well as some other information about their interests, etc. After that, the teacher should discuss with students what is considered oversharing.

What is Considered Oversharing on social media?

Oversharing on social media is based on exposing intimate details about your personal life such as relationships, friendships, family matters, or your daily routine. Some examples include:

- Regularly posting who you are with

The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

- Posting intimate details about your relationships, friendships, family members and personal drama
- Enabling the geographic location on every post
- Constantly posting pictures of what you are wearing
- Posting work-related information on your account

After talking about oversharing on social media, the teacher tells the students to write 2 possible dangers that can happen if they overshare their personal life. Give them about 10 minutes and let them search the internet for some issues that happened recently regarding online bullying, identity theft, etc. Encourage them to think as inspectors and to think outside the usual box of typical digital threats.

Possible answers that are interesting for further discussion:

- Account Takeover
    - A cyberattack wherein cybercriminals utilize usernames and passwords that have been stolen to seize control of online accounts.
- Social Engineering
    - Social engineering is the psychological manipulation used to get others to do things or reveal private information. This method is often seen through phishing emails.
- Reputation
    - Protecting the reputation of who you are in your personal and professional life could be jeopardized if you overshare a bit too much in your accounts.

The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

After students read what they have written, a teacher can start the small discussion about who can see their personal information and what can they do with it. It's really good to encourage the debate about the pros and cons of sharing our life on the internet as well as focus on some particular bad praxis that students found on the internet regarding identity theft, bullying, etc.

The teacher can also mention cookies on websites and explain to them in which way they can be manipulated on the internet and see what they think about it. The idea behind this is to encourage students to think more critically about their digital identity and the real dangers of excessive sharing of personal information.

The discussion should last ten to fifteen minutes and the teacher should be a moderator and shouldn't bring any conclusions by himself. Also, it is important to encourage students to share some personal negative experiences on the internet and to feel safe in classroom surroundings. In this case scenario, it is important to build trust in the classroom and encourage understanding without judging anyone or anything. The conclusion in that case scenario should be towards understanding that sharing their experience in safe surroundings like a classroom, with family or close friends is better than sharing sensitive information on the internet.

3.2. Part II. Why do we have a right to privacy?

The teacher/facilitator presents to his students a short text regarding the surveillance system in China which has become a popular topic in western media:

The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

"Security cameras automatically capture the people's faces, and match with house rental information, records in hospitals, hotels, and school, and summarize an activity log of different groups of people. With all information and data collected, an alarm model would be created to automatically identify abnormal activities."

Just exactly how the model will be implemented is not yet known. But combined with China's existing surveillance system, the Sharp Eyes project could allow community workers to proactively go to individuals' doors to investigate a crime that has not even been committed yet.

Its goal is to create a system that is literally meant to "prevent crime before it happens."

Firstly, the teacher must give students some short time to think about the written and then he should follow a set of questions that can encourage students to think philosophically about the subject. Every question can guide to more questions and a broader discussion but should follow this structure:

- Is it justified to track the individuals for a greater cause and why do you think that way?

    - In which cases you would allow your state to surveil you?

    - Do you think it would prevent something from happening

- Is it more important for a human being to be safe or free?

    - Can you project the negative influences of this kind of surveillance system in near future?

    - Do you think that society is a slave of technology or do you think the opposite?

The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

- How many people can see your own location or your behavior on social media?

    - Has anyone ever judged you on social media or have you ever heard of something similar?

    - What is the difference between the Chinese new surveillance system and everyday life of a western man?

- Do you know in which way can your personal digital data be used?

    - Have you ever actually read the terms and conditions on any web site?

    - Do you think it's risky to let companies track your every step in a digital environment?

- Do you know how many websites and mobile apps have your personal data?

    - Can you name some of them?

    - Does a modern human being have a right to privacy or freedom and if he does, in which way he can use it?

    - Can technology, digital environment and artificial intelligence change human nature?

Every question can be followed by a set of sub-questions to help students to scratch further or to encourage them to discover the new meanings behind the concepts they are already familiar with. It is the Socratic maieutic method in which the teacher doesn't give

The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

their students the definitions or some meaningful conclusions but tries to encourage students to grasp into already known concepts and facts that surround them and by which they act and think. For example, they can talk about the modern concept of freedom or they can discuss various problems of society regarding the relationship between a human being and a machine (artificial intelligence, etc.). An open dialog is necessary for the success of this approach to the workshops.

4. DISCUSSION CHECK

As this workshop is built completely on a set of discussions, the next questions can be used to expand on the topics explored through the course of the workshop and guide the workshops to different conclusions and a broader picture of the topic:

1. How do you think the world will look like in 10 years if artificial intelligence takes over some aspect of human life?
2. Do you think that humankind is more powerful than technology?
3. What would your life be without social media?
4. Imagine one week without technology and tell us what could you do that week?
5. Is privacy more important than world peace?
6. If the whole world would be under surveillance, do you think it would be a better or a worse world to live in?
7. Why do people overshare their personal life?
8. Is it better to be mysterious or to be completely open to the world?
9. Is anyone in the classroom completely off of social media?
10. Do you feel that people who are really active on social media are in some kind of advantage or disadvantage towards others?

The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

5. ADDITIONAL RESOURCES

- Online article “Digital privacy in education” [https://ecampusontario.pressbooks.pub/digitalprivacyleadershipandpolicy/chapter/digital-privacy-in-education/]
- Online article “Inside China's Surveillance State, Built On High Tech And A Billion Spies” [https://worldcrunch.com/culture-society/china-surveillance-cameras]
- Online article “How Oversharing on Social Media Affects Your Privacy“ [https://www.keepersecurity.com/blog/2022/12/23/how-oversharing-on-social-media-affects-your-privacy/]
- Online article “Four Takeaways From a Times Investigation Into China’s Expanding Surveillance State” [https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html]
- Online article “Surveillance State explores China's tech and social media control systems” [https://www.npr.org/2022/09/07/1118105165/surveillance-state-explores-chinas-tech-and-social-media-control-systems]
- Online article “7 Examples of Data Misuse in the Modern World” [https://www.invisibly.com/learn-blog/data-misuse-7-examples/]
- Online article “Philosophy and Digitization: Dangers and Possibilities in the New Digital Worlds” [https://www.degruyter.com/document/doi/10.1515/sats-2021-0006/html?lang=en]
- Book: Soames, S. *The World Philosophy Made: From Plato to the Digital Age* Princeton University PressOnline, 2019

The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project’s national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

- Youtube video “How China’s Surveillance Is Growing More Invasive | Visual Investigations” [https://www.youtube.com/watch?v=Oo_FM3mjBCY]

6. ANNEX

Threats to Your Social Media Accounts:

It is time to start taking social media seriously. Below are three common threats that individuals fall for when it comes to protecting their accounts. Being aware of the following can decrease your chances of becoming a victim.

- **Public Wi-Fi**
  - Logging into your social media accounts on an unsecured public Wi-Fi network puts you at risk of somebody intercepting your data. One of the most prominent cyberthreats to public Wi-Fi is a man-in-the-middle (MITM) attack. This attack relies on network manipulation, or the creation of malicious networks, under the control of cybercriminals that operate as “middlemen” between the sender and the recipient of information, altering the traffic and intercepting data.
- **Phishing scams**
  - Phishing scams are when a cybercriminal tricks you into giving them your login information by sending you messages, usually through email, that look like they’re from a trustable source asking to confirm your login credentials or provide them with private information. For example, a phishing scam can

The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project’s national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

look like it's coming from a platform such as Instagram asking you to reset your password using a malicious link.

- Clicking on links in emails or messages that are unfamiliar or unexpected, even if they appear to be from a trusted source, should be avoided at all times.

- **Weak passwords**
  - If you use a weak password for all your accounts, it is much easier for a cybercriminal to guess it based on the personal information that you have overshared such as your dog's name or birthdate. Always use a strong password in order to protect your privacy.

What Can You Do to Prevent Oversharing on Social Media?

You can prevent oversharing on social media by being more thoughtful and following different security best practices. A good rule of thumb is to consider if something is appropriate as a public post or if it's better as a private message. It's also important to differentiate between platforms you want to use privately and professionally, as this allows you to post adequate content without jeopardizing your professional reputation.

We recommend that you switch to private accounts when possible and turn on 2-step verification to further secure your accounts. Make sure that you accept friend requests only if you truly know the individual and determine whether it is appropriate for them to see your content without putting yourself at any risk.

The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

Personal digital data gets used in one of three ways:

- Personal data is aggregated and analyzed to provide us with more personalized advertisements.
- Personal data is logged and assessed for research and development.
- Personal data is sold to a data brokerage.

The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.