
Munich Personal RePEc Archive

Workshop report: Creating a citizens' information pack on ethical and legal issues around ICTs: what should be included?

Asine, Janice and Baibarac-Duignan, Corelia and Broglio, Elisabetta and Castañeda, Alexandra and Feord, Helen and Freyburg, Linda and Leppée, Marcel and Matheus, Andreas and Camara Oliveira, Marta and Pavlakis, Christoforos and Peira, Jaume and Soacha, Karen and Thuermer, Gefion and Vohland, Katrin and Wagenknecht, Katherin and Woods, Tim and Zourou, Katerina and Caruso, Federico and Duerinckx, Annelies and Klimczuk, Andrzej and Sterken, Mieke and Berti Suman, Anna

2020

Online at https://mpra.ub.uni-muenchen.de/108777/
MPRA Paper No. 108777, posted 23 Jul 2021 05:04 UTC

Creating a citizens' information pack on ethical and legal issues around ICTs: what should be included?

Workshop report

9-10 March 2020
Museum für Naturkunde Berlin

cost
EUROPEAN COOPERATION IN SCIENCE & TECHNOLOGY

Funded by the Horizon 2020 Framework Programme of the European Union

Background to the workshop

The workshop was organized through a collaboration between: the European Citizen Science Association (ECSA), COST Action 15212, the Institute of Marine Sciences (ICM-CSIC), and the PANELFIT and EU-Citizen.Science projects. This collaboration was led by Jaume Piera, Karen Soacha and Federico Caruso (PANELFIT), Tim Woods (EU-Citizen.Science and PANELFIT) and Katherin Wagenknecht (EU-Citizen.Science). Financial support was provided by PANELFIT (EU grant agreement 788039) and COST Action 15212 (supported by European Cooperation in Science and Technology). Helen Feord of ECSA was responsible for note-taking and writing this report.

The call for participants was made available through the COST Action 15212 website, and promoted through the organizers' networks. To increase the diversity of participants, in terms of backgrounds, fields of interest and expertise, some people were specifically invited to apply.

Unfortunately the workshop coincided with the start of the COVID-19 outbreak in Europe. As a result, not all of the invited participants were able to travel to Berlin. To allow for their inputs, this report has been produced using a two-step process: (1) drafting the report from the meeting notes made in Berlin, and (2) inviting all participants to make further inputs after the event.

Despite this setback, 17 participants met in Berlin (see Annex 1), representing 11 countries and drawn from the fields of academia (including PhD students and early-career researchers), citizen science, citizens' groups and the private sector. A further five participants (representing four countries) contributed virtually.

Workshop aims

The aim of this workshop was to ask potential end-users of the citizens' information pack on legal and ethical issues around ICTs (i.e. citizens and citizens' groups) the following questions:

- What is your knowledge of the EU's General Data Protection Regulation (GDPR), and what actions have you taken in response to these regulations?
- What challenges are you experiencing in ensuring the protection and security of your project data, and compliance with the GDPR, within existing data management processes/systems?
- What information/tools/resources do you need to overcome these challenges?
- What are the best formats/channels for receiving, sharing and acting upon this information?
- What is the most appropriate structure/format(s) for the citizens' information pack?

This workshop supported the aims of Working Group 5 of the COST Action 15212[1] by contributing towards a framework - namely, legal and ethical requirements for citizen science projects, and the data they collect, store and share - for "the exploitation of the potential of European citizens for science and innovation".[2]

The end product of the process - the citizens' information pack on legal and ethical issues around ICTs - will "identify and enhance good practices that can be applied to citizen science projects in different areas"[3] and support efforts to "explore ways for integrating data and knowledge collated through [citizen science] initiatives and suggest mechanisms for standardization, interoperability and quality control".[4]

The workshop was planned so that it would guide the final content and style of the citizens' information pack on ethical and legal issues around ICTs, which will be developed through the PANELFIT project, and to ensure that this meets the needs expressed by citizens and citizens' groups. We aim to verify the findings of this workshop through an online survey, to ensure the views of further citizens and representative groups, including those from other backgrounds and context, are also represented. These findings will be fed back to PANELFIT's Engagement, Communication and Dissemination Board, which will draft an editorial plan for the citizens' information pack.

In preparation for this workshop, participants were asked to:

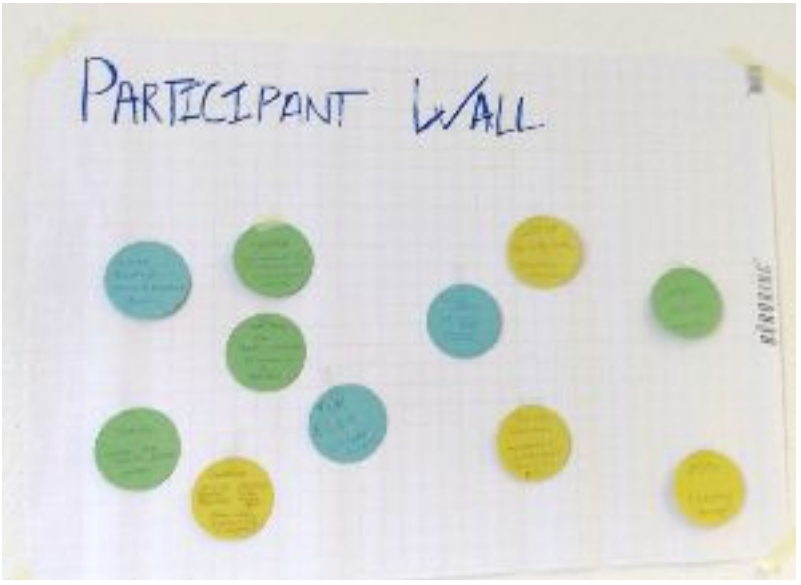
- familiarise themselves with the PANELFIT and the EU-Citizen.Science projects
- identify 2-3 challenges they experience in data protection and security, or the projects/groups they work with experience, and what they would like to know about overcoming these
- read the paper on data and citizen science by Quinn (2018)
- read the paper on vulnerable groups by Peroni and Timmer (2013).

[1] This is the 'Improve data standardization and interoperability' Working Group.
[2] p3, www.cs-eu.net/sites/default/files/media/2017/04/CA15212-MoU.pdf
[3] Ibid.
[4] Ibid.

Session 1. Project and participant introductions

During the opening working lunch, the participants were asked to create a profile on the participant wall (see Figure 1). This is an interactive method through which people can find out about each other's experiences and knowledge, and how they overlap with their own. After this, the organizing projects and institutions were presented.

Figure 1. The participant wall



Session 2. Common language and shared definitions

This participatory session aimed to create a shared understanding and definition of some terms relevant to the workshop's aims. Given participants' differing nationalities, cultural backgrounds and first languages, this was an important prerequisite for later discussions. Participants were invited to offer a definition for each term, with others then strengthening or challenging this. The words were written on separate sheets of paper and placed on the wall, where they remained as reference points for the rest of the workshop.[5] Some of the main discussion points are captured here.

Personal data

This broad concept was identified as being a fundamental right: one which includes preventing access to it (data) by others. In the context of this workshop, a key question raised was: how do you prevent putting citizens at risk when working with their personal data?

Data management

Data management includes data collection, maintenance, use, sharing and storage. It involves looking at the lifecycle of data processing, as well as the tools which are used for data maintenance (i.e. using tools developed externally and those made by the user). Existing tools require policies that ensure fair and consistent use (e.g. to establish why, what, when, where, who has access to the data, for how long).

In citizen science, data management involves looking at the whole project: from the planning phase, and then throughout its duration, in order to protect citizen scientists' data in the best way possible.

Different types of data, such as metadata and offline data, require specific data management policies. Questions on these categories included:

- What are the ethical and legal implications of considering metadata in studies?
- Which parts of the metadata should be visible, and which should be invisible?
- How does the management of offline data compare to that of online data?

Data re(use)

Subjects covered under this theme included a discussion around the need to enhance (re-)use through, among other approaches, applying the FAIR principles.[6]

Data protection

Data protection[7] should work to this principle: 'Nothing happens to my data that I did not

[5] As a group we agreed to defer the definition of 'vulnerable people' until Session 5.
[6] FAIR data are data which meet principles of findability, accessibility, interoperability and reusability.
[7] This discussion focused mostly on data protection in a European context, and from (mostly) European perspectives. For a wider view on data protection, see: https://globaldatajustice.org/

give permission for'. Discussion points around this term included the need to define who the data controllers are, and that data should be protected from being publically available, with access only given to those who require the information. An illustration of this came from the field of conservation and protecting endangered species; for example, data on i-Spot might be used by illegal loggers or poachers trying to locate species to fell or hunt. Another point raised was the need to think about how to acknowledge people - a key tenet in citizen science - while protecting their privacy; this was seen as complicated, but doable.

Security/cybersecurity

The initial debate focused on whether security and cybersecurity could have a joint definition. From a citizen science perspective, it could appear that cybersecurity is not important, as cybersecurity mainly ensures websites or apps are not hijacked. However, because many citizen science projects use the internet, understanding the risks of this for citizens is very important. It is important to identify the challenges associated with any system and to test them. It is also necessary to consider different levels of vulnerability and risk in terms of cybersecurity. There are two further perspectives to take into account here: that of the developers (e.g. of a citizen science app or website) and that of its users. Good practice is required on all sides.

GDPR

The discussion here centred on whether there should be an exception for the application of the GDPR in the context of citizen science. Caveats already exist for university/research institute guidelines, so application of the GDPR in some instances is already balanced against more general guidelines. In terms of applying the GDPR to open science and citizen science, it would be beneficial to have more tools to deal with this, as it is a complicated process.[8] 'Data governance' was highlighted as a term which should be part of the conversation.

Session 2 conclusion

These definitions do not provide a 'final word' on these terms, even within the field of citizen science. However, the considerable debate (and disagreement) generated among participants is telling: it implies that, even among people working largely in the same field (citizen science), there is not always a shared understanding of all the terms around data protection and ethical and legal issues around ICTs. There is likely to be even greater disagreement among citizens more widely. This suggests there is a real need for clear definitions of key terms to be part of the citizens' information pack.

[8] Suman and Pierce (2018) discuss this in more detail. See: https://edpl.lexxion.eu/article/EDPL/2018/3/7

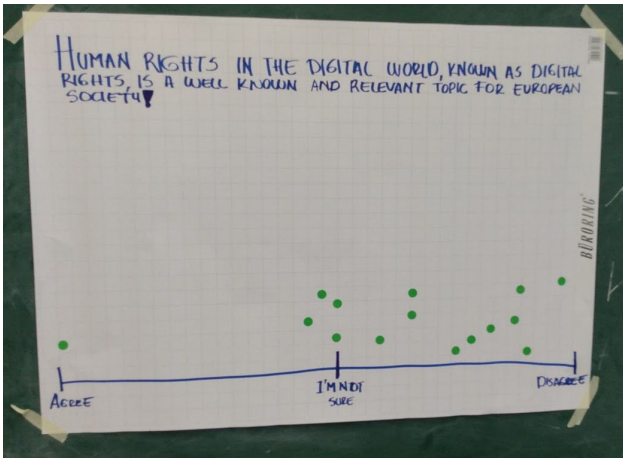
Session 3. What do we know about data protection and security?

Session 3 was an interactive session to discuss and challenge some key perspectives and positions around data and ICTs. Five sentences were written on flipchart paper. Below each statement was a scale ranging from 'Agree' through 'I'm not sure' to 'Don't agree'. Each participant was given stickers to add along this scale, to indicate their position on the statement. This was followed by a group discussion to explore the trends identified.

Statement 1: Human rights in the digital world, known as digital rights, is a well-known and relevant topic for European society.

Most people disagreed with this statement: they felt that most people are not interested in this topic and do not consider it as relevant. However, there was an outlier at the opposite end ('agree'), who stated that while it may not be well known, it is extremely relevant to society. This led to a debate about whether 'well known' and 'relevant' should be treated separately within this statement.

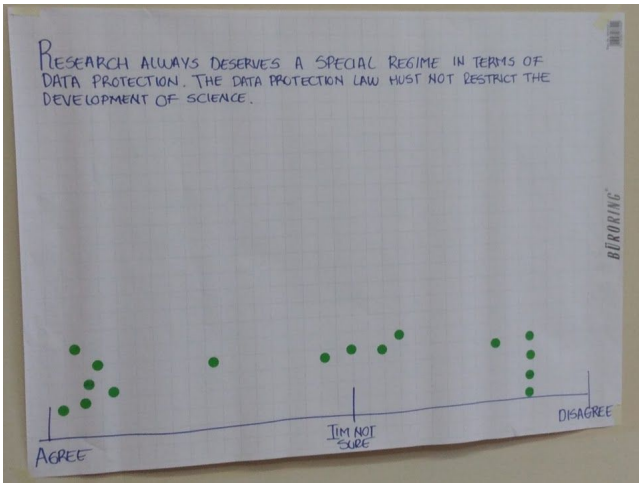
Figure 2. Responses to statement 1



Statement 2: Research always deserves a special regime in terms of data protection. The data protection law must not restrict the development of science.

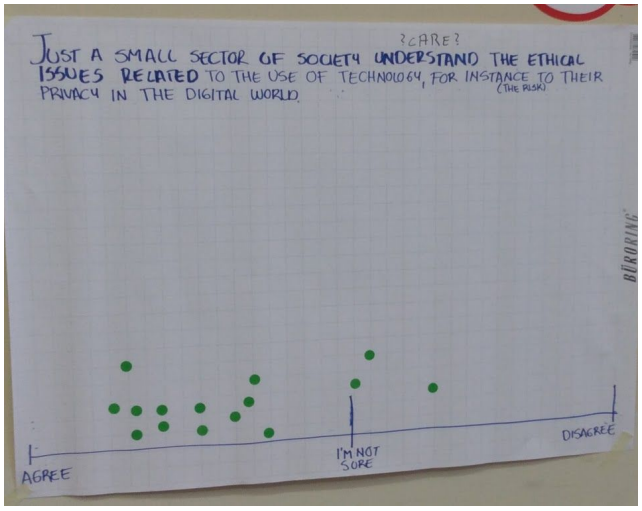
For this statement, opinions were split. Those in agreement felt that because research data can be very sensitive, data protection laws could be adapted to the context - but agreed that data protection remains fundamental to the ethics of science. One option would be to divide research into two types: open access research and restricted research (i.e. restricted due to safety concerns). Another suggestion was to look at this question from the opposite perspective: how can science apply the law fairly? Maybe the notion of 'difficulties' could replace 'restrictions'?

Figure 3. Responses to statement 2



Statement 3: Just a small sector of society understands (or cares about) the ethical issues related to the use of technology, for instance (the risk) to their privacy in the digital world.
Before placing their markers along the scale, participants clarified the statement (adding the text in parentheses). A majority agreed with this revised statement. It was suggested that language used to explain these issues could be a barrier (e.g. if it was too technical) and that this should be addressed in the citizen's information pack to be produced by PANELFIT.[9]

Figure 4. Responses to statement 3

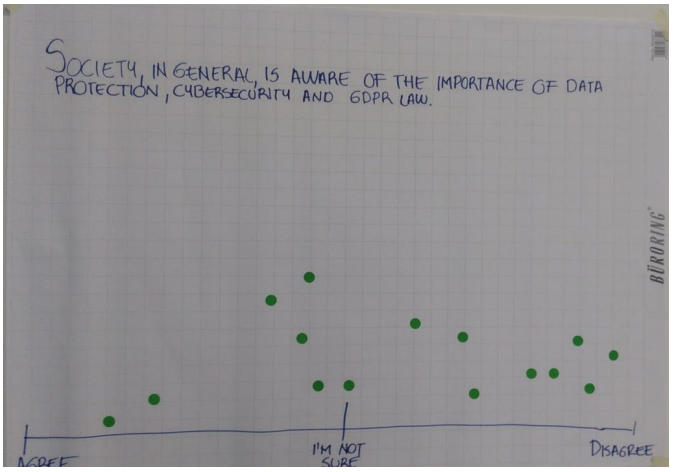


Statement 4: Society, in general, is aware of the importance of data protection, cybersecurity and GDPR law.
This statement drew the most dispersed responses. While there was a tendency towards 'disagree', many participants were unsure and some agreed with the statement. This variance was unpacked during the discussion. One explanation was that while many people

[9] The issues raised in this statement are not exclusive to Europe. See, for example, Milan and Treré's (2017) discussion of Big Data in the South: https://data-activism.net/2017/10/bigdatasur/

are aware of these issues, they may not understand them. Therefore, finding a simpler, more efficient way of putting data protection guidelines into practice was recommended. Again, this confirms that the PANELFIT project is meeting a clear need.

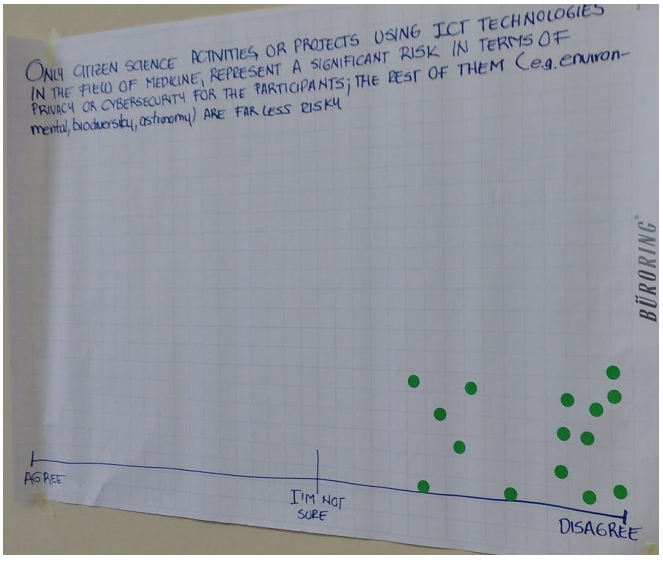
Figure 5. Responses to statement 4



Statement 5: Only citizen science activities, or projects using ICT technologies in the field of medicine, represent a significant risk in terms of privacy or cybersecurity for the participants; the rest of them (e.g. environmental, biodiversity, astronomy) are far less risky.

For the final statement, there was a strong consensus towards 'disagree'. For example, in contexts where environmental activists can be exposed to legal risks (such as strategic lawsuits against public participation, or SLAPPs), there are privacy and cybersecurity risks. It was agreed that this is a statement of principle applicable to all fields, and therefore not only relevant to the context of (citizen) science.

Figure 6. Responses to statement 5



Session 3 conclusion

The sample size and diversity of participants, and the targeted selection process (i.e. participants invited through citizen science communications channels, and experts invited to provide particular inputs) was too small for the responses to these statements to be anything more than indicative. However, the responses given suggest that there are still discussions to be had around these issues, and that many debates around data privacy and ethical/legal issues remain far from resolved. In particular, statement 2 highlights that there is not yet agreement on how data protection laws should be applied to research.

Session 4: Mapping challenges and solutions

In this interactive session, participants were asked to identify personal and organizational challenges related to the legal and ethical aspects in the use of ICTs - and to outline any solutions they have come up with to date.

Participants worked in three groups to answer the following questions:

- What are the main challenges/issues/tensions related to ethical and legal aspects in ICTs that we need to make easier to understand, especially with respect to vulnerable people?
- Is there any specific group of society affected by these issues/tensions?[10]
- How can we tackle these challenges through the citizens' information pack?

Table 1 summarizes the results from this exercise, with the responses from each group collated. Post-workshop suggestions and clarifications are in italics. All results were subsequently grouped, post-workshop, by Annelies Duerinckx and her colleagues.

Table 1. Mapping challenges, vulnerable groups and solutions

1. What are the main challenges / issues / tensions related to ethical and legal aspects around ICTs?
Communication ● There are challenges in making legal and ethical aspects easy to understand (*e.g. as guidelines, toolkits, textbooks, best/good practice examples, etc.*). ● There is a lack of interest in GDPR (*or rather, insufficient interest*). ● People do not (always) read terms and conditions, privacy policies, etc. ● Citizens must have a say on how their data is to be used (*i.e. there is a need for two-way communication*). ● There is a need to explain to people how and when it [data protection] affects them. ● How can we make certain people aware of the availability of the citizens' information pack (e.g. offline communities)? ● Citizens have doubts about their rights, and who to ask about this. ● Debates around this subject are inaccessible for non-experts (i.e. people cannot comprehend them). ● Language is a barrier in communicating people's rights, including non-European languages spoken in Europe (e.g. Farsi). ● *There is a need to explain to people (citizen scientists) about their data and their protection (rights).* ● *Accessibility: where is information about peoples' right available, and how can they get this?*

[10] Annex 3 provides a list of vulnerable groups identified through this workshop, and from other sources.

Inclusion

- There is an need to focus on vulnerable groups, but:
    - the nature of vulnerability varies (e.g. financial barriers, health- and capacity-related barriers, location-based barriers such as rural areas)
    - vulnerability is not (just) related to a specific group, but also the kind of data (e.g. religion, medical history, sexual orientation) and the context.
- One challenge is how to make scientists aware of the legal and ethical issues applicable to vulnerable groups.
- How can we open up citizen science processes (e.g. data collection) to low-tech (vulnerable) participants?
- There is a need to reach out to offline communities; there is a role here for intermediaries / mediators to help search for and reach these groups.
- Different groups (e.g. age/education/gender) have different needs - and they all overlap the digital divide.
- "Empowerment versus the dark effects of vulnerability".
- *There is insufficient access to resources (e.g. funding) for scientists to do community intervention and reach out to people.*

Diversity

- *What about community-led science? How can ICTs and privacy regulations deal with this?*
- *Different groups have different needs (e.g. age, education, gender, location, finances, health).*
- *Different types of data have a different degree of vulnerability (e.g. religious data, medical history, sexual orientation).*
- *The context of the data retrieval differentiates the needs.*
- *How to handle dynamic changes in data rights?*

Missing/important information

- Regarding the degree or type of personal data needed: what is the boundary?
- *What should we do if someone uses our personal data in an inappropriate way?*
- Is there a difference between consent and informed consent?
- Metadata: what do they contain?
- Data portability:
    - Do we have to ask again? (researcher)
    - Do I have to give consent about this again? (citizens)
- There is a tension between the potential use of my personal data and the misuse of my personal data.

Existing paradoxes and uncertainties

- There are different interpretations of GDPR in different countries.
- Data rights change: applying these is a dynamic process.
- Ethical and legal issues / implications of data use (i.e. developments) will also change.
- The ownership of the data is an ongoing challenge.

- *Intellectual property and copyright: data = money, and some people/groups/organizations etc. can gain financial or other benefits from the use of data.*
- Tension: the acknowledgment of contributors in citizen science versus privacy rights.
- Publication of research data (Open Access) <--> Data protection.
- How do we treat sensitive data that is not personal data?
- There are ethics around revealing/protecting certain data (e.g. on the occurrence of endangered/rare species) to protect them from abuse of knowledge. This contrasts with the tendency to make data open and linked.

2. Is there any specific group of society affected by these challenges / issues / tensions?

- Offline communities
- People with limited knowledge of technology / digitally illiterate
- Those with limited access to infrastructure
- Research teams that are under-resourced
- Communities who remain outside of the research process, but who we need for more community-led science to happen
- Older people
- LGBTQ+ people
- Illiterate people or those with low literacy / education
- Indigenous communities: there are risks concerning their traditional knowledge and how they understand their relationship with this issue (data protection and rights)
- People excluded by language / people who are not fluent in English
- Migrants, especially those who do not speak the local language
- Children / minors who cannot legally consent to the use of data
- Visually impaired / blind people using software that reads the screen / platform to them (lower privacy)
- *Homeless people*
- *Unemployed people*
- *Refugees*
- *Social care clients/beneficiaries*
- *Single parents or guardians of dependent persons*
- *People with learning difficulties (e.g. dyslexia, dysorthography, dysgraphia, dyscalculia)*
- *Persons who do not speak the language of the country of residence (foreigners/expats)*
- *Patients and long-term patients*
- *Prisoners and persons leaving prison*
- *Representatives of minority groups (e.g. sexual, religious, ethnic)*

3. How to tackle these challenges through the citizen's information pack?

- Include forms / templates to communicate concerns to researchers.
- Standardized T&Cs/privacy policies for citizen science that are easy to understand for everyone.
- Enable co-creation to reflect power balances and inequalities.

- Bring the citizens' information pack into the hands of these groups and the relevant intermediaries / mediators.
- Find mediators and intermediaries for vulnerable groups: they need to talk to people that they trust.
- Create a directory of local NGOs / ambassadors with analogue channels for reaching people not in the digital world.
- Make data readable for citizens who contributed to a citizen science project.
- Be clear by using common language and concept about digital rights:
    - Simple, plain language = inclusivity
    - Something accessible: not too overwhelming, not too technical
    - Visual representations of difficult (legal) concepts.
- Use citizen science and gaming to communicate - but only users that already use your citizen science game; it's not ethical to encourage people to start gaming.
- Use short YouTube tutorials (max. 2 minutes).
- Answer the "so what" questions; why should people care in the first place?
- Identify the people / websites / institutions responsible for clarifying doubts.
- Address 'information poverty' by designing inclusive information systems.
- Create training, guidelines, materials for legal communities.
- The citizen's information pack must be accessible (e.g. for blind, deaf people); ideally, it will follow the Web Content Accessibility Guidelines, which set the main international standards for the World Wide Web and its accessibility.[11]
- Have the information in different languages.
- Provide best practices for researchers.
- Provide testimonies from citizens, and interactive spaces for sharing best practices.
- Identify existing clear guidelines on data use; Natura 2000 / ProtectNatural Park are good examples.
- Have a clear strategy for dissemination of the citizen's information pack (e.g. through libraries, civic centres).
- Use visual communication (e.g. diagrams, checklists).
- Use examples and case studies to show the importance of the use of data.
- Include small interviews with users/citizen scientists of why it is important to take care of data.
- It should be a living document, available through different websites (e.g EU-Citizen.Science, PANELFIT).
- Try and explain fewer concepts - but more efficiently.
- *Offer help desks for people with further questions.*

At the end of the day, an exercise was distributed in preparation for session 5. This allowed the participants to begin discussions around vulnerable groups during the evening meal for participants, which enabled us to move beyond discussions and reach conclusions during this session in Day 2.

[11] See: www.w3.org/WAI/standards-guidelines/wcag/. Further information from ICT4IAL on Web Accessibility Checkers, and a tool related to photosensitive epilepsy analysis, are available from: www.ict4ial.eu/what-meant-accessible-information.

Session 4 conclusion and daily wrap-up

This session was vital for identifying and explaining the challenges that the citizens' information pack needs to address, especially for those people particularly affected by ethical and legal issues around ICTs (a theme continued in session 5). It also began the critical process of compiling possible content for the citizens' information pack, along with ideas for how best to present and share this.

Session 5: Vulnerable populations in Europe

This session was split into two parts: a walkshop and a plenary. A 'walkshop' is an interactive methodology used (and possibly created) by the Institute of Development Studies in the UK. The aim is to break up the typical workshop format of sitting in one room, and enable participants to walk around a particular area with a set theme to discuss. The advantages of this method are numerous.

- It provides an opportunity to gain some exercise, and see a little more than just the workshop venue/room, which can help to invigorate participants for the remainder of a workshop.
- It is a way to allow people to speak to 'new' participants, other than those they already know or are sitting with.
- Conversations are in smaller groups, meaning those who haven't always been heard in larger groups have a space to share their ideas and opinions.
- Taking people away from distractions (e.g. phones, emails, laptops) helps to focus them on a specific topic.

Participants were invited to walk around the Museum für Naturkunde for one hour and discuss the topic 'Vulnerable populations in Europe', focusing on the questions provided the night before (see subsections below). Participants were encouraged to keep notes from their discussions to share in a plenary. This was also an opportunity for the participants to visit the museum and take advantage of being in Berlin.

The second part of the session was a plenary discussion to feed back ideas and opinions that had come up in conversations, as well as anything else of relevance to the workshop themes. The following text summarizes the outcomes of these discussions.

1. Who can be seen as 'vulnerable' in Europe?

Building on the groups identified during session 4, participants identified the following as vulnerable (or potentially vulnerable) within Europe. [12]

- People who are under-educated and poorly educated.
- People who are outside of a training/education system (especially the 15-18 age group).
- People who are misinformed, including those who may not be able to understand the information provided.
- People who are illiterate, including digitally illiterate
    - It was also noted that certain people are more digitally connected, but might come from another group that is vulnerable, and their digital literacy does not remove this vulnerability.

[12] While our focus was on Europe, it is noted that many research projects extend beyond Europe, and therefore further non-European vulnerable groups may need consideration.

- People who are unemployed (or underemployed) and/or who have low-economic status
- Emerging adults (20-30)
- People belonging to the 30-40 age group, who may be unemployed or have a low income:
    - Many people in this age group in certain countries (e.g. Portugal, Netherlands) tend to be self-employed or freelancers, who especially during moments of crisis (such as the current COVID-19 pandemic) are vulnerable to dramatic changes in income.
    - They may also have young families, and hence have an increased level of vulnerability (e.g. financial).
    - Conversely, they may potentially have higher levels of technical skills and education than other age groups.
- People with language barriers / networks (e.g. Creole speakers in Portugal).
- People with disabilities, either physical or mental, and both permanent and temporary.
- Indigenous groups, who require the protection of their heritage (e.g. in museums).
    - We need to take into account provenience data (from provenance research on the origin, ownership and custody of objects) and people's knowledge, which may be stored without their knowledge or approval.
- Members of the Roma community.
- Migrants.
- Refugees.
- People hit by phenomena beyond their control, such as extreme climate events.

This list has been added to Table A1, which draws on other sources to move towards a comprehensive set of vulnerable people in Europe. However, the workshop participants also noted that in addition to these vulnerable groups, we should also consider any citizen, who for any reason considers themself to be vulnerable and looks for support in this respect.

2. Which specific ethical and legal challenges do these groups face, in terms of ICTs and data?

Here, discussions moved away from allocating specific challenges to specific vulnerable groups. Participants suggested this was too simplistic and could lead to 'box-ticking'. A more useful approach - and a more useful role for the citizens' information pack to play - would be to lead its end-users (including researchers, citizens, citizen science practitioners) to consider the nature of vulnerability. The following concepts were considered with respect to the term 'vulnerable'.

- **Static versus dynamic**: vulnerabilities can change in nature over time, or new vulnerabilities can manifest (or become redundant). Individuals or groups who are not vulnerable at the start of a research project may become so during its lifetime.

- **High versus low**: the severity of a certain type of vulnerability can change over time, due to changing personal circumstances (e.g. increasing / decreasing resilience) or external ones (e.g. the causes of the vulnerability intensify or lessen); it can also vary within a vulnerable group (not all individuals experience the same levels of vulnerability).

This discussion highlighted that 'vulnerable' is a complex term. In this regard, vulnerability should be seen as a spectrum: individuals or groups can have high or low levels of vulnerability, which can be fixed (static) or changing (dynamic). It was also noted that everyone is potentially vulnerable, and that their level of resilience, access to resources (e.g. infrastructure) and certain cultural factors (e.g. support networks) are determining factors.

The conclusion was that we should consider the definition of 'being vulnerable' as dynamic. Contexts which could influence people's vulnerability include:

- their cultural heritage being under threat, or their access to it being under threat
- external threats such as climate change (e.g. in polar regions, Scandinavia), and associated events such as heatwaves and floods
- people's resources being vulnerable, such as language, families and networks, and their natural heritage.

3. How can their rights be better supported?

Time became limited at this point, meaning less time was available for the two final questions. However, there was a suggestion to use the EU-Citizen.Science to crowdsource solutions to this question, and to support people's efforts to educate themselves on the topic.[13]

4. What needs to be included in the citizens' information pack tailored to vulnerable groups?

Building on the ideas in session 4, there were several suggestions.

- It should include guidelines on addressing different types of vulnerability: how to support people to overcome this.
- There should tools to help people think beyond who they immediately see as vulnerable people.
- It should not aim to provide ideas specific to a few vulnerable groups, but address the common issues that such groups face.

[13] A potential resource for this is a mass open online course (MOOC) about GDPR from the National Public Administration Institute in Portugal, which is targeted at citizens who want to know more about these issues (in Portuguese): https://lms.nau.edu.pt/courses/course-v1:INA+RGPD-CA+2019_T2/about

Session 5 conclusions

It was not our expectation, nor our intention, to provide simple solutions to the particular challenges facing vulnerable populations with respect to ethical and legal issues around ICTs. Rather, the exercises held aimed to begin the process of 'unpacking' vulnerability in relation to these issues, given its inherent complexity - a complexity reflected in the fact that three attempts to list Europe's vulnerable groups produced three different, if overlapping lists (during Session 4, Session 5 and contributions by offline participants). The complex nature of vulnerability is further exemplified by the full list of groups, which is compiled in Table A1.

Participants identified many other factors that make the issue of vulnerability resistant to simple analysis and solutions.

- People may belong to two or more groups, making the nature of their vulnerability even more complex. Among older people, for example, some are well educated and some are poorly educated, both in general and in terms of digital literacy; many live alone or in nursing homes, which may increase the likelihood of them being digitally illiterate compared with the wider older population.
- Some categories of vulnerability are based on ethnicity or geography, while others on transversal traits, such as changing employment situations.
- Some are not consistent in form across a group; disabilities, for example, can be permanent or temporary.
- Certain groups need careful definition and even sub-categorization; for example, 'younger people (16-25)' is too broad, and should be broken down into (as a minimum): school students; those in higher education; those in employment (permanent or insecure); those outside of education and employment.
- There is a temptation to assume characteristics for certain groups that are not correct or consistent. For example, some refugees may be well educated and speak English well (or the native language to their host country); but they may, as with other refugees, lack access to computers, employment etc.

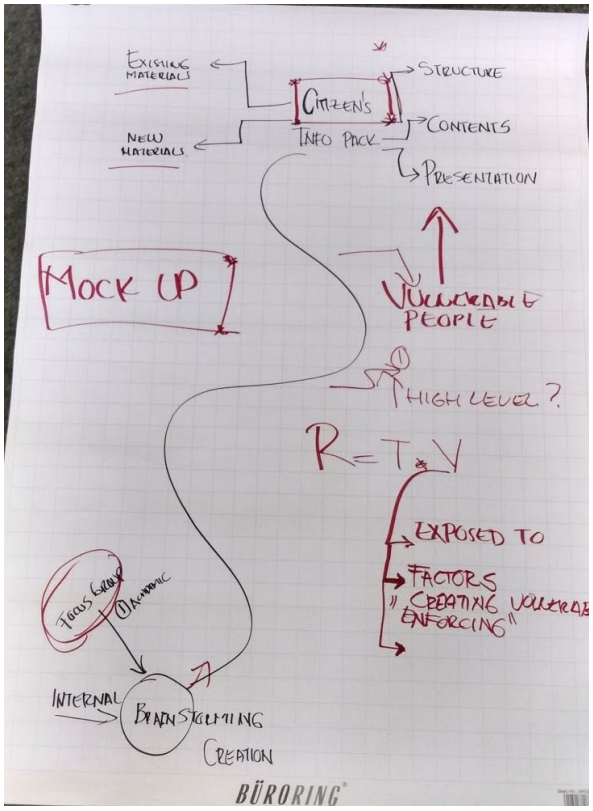
In terms of looking for concrete solutions to ensure their data (and other) rights are met, it may be easier to consider vulnerable groups in terms of all the barriers they encounter, and then focus on strategies for overcoming each barrier separately, rather than seeking to identify or create 'solutions' for each vulnerable group.

Session 6: Prioritizing and designing solutions

To conclude the workshop, participants were asked to create a mock-up of how they envisaged the citizens' information pack looking, in terms of content, presentation and structure. This was done using their own knowledge and experience, and ideas generated during the workshop.

Figure 8 shows the visual aid used to show where this task sat along the path, from initial brainstorming to the final output. Beyond this, however, the workshop organizers, several of whom are responsible for creating the citizens' information pack through the PANELFIT project, did not provide too much detail about what it might look like. This was a deliberate decision to allow for new ideas (i.e. outside of our own) to come forward.

Figure 8. Pathway to the citizens' information pack



Figures 9-12, on the following pages, provide outlines of the mock-ups that each group devised.

Figure 9. Group 1 mock-up of the citizens' information pack

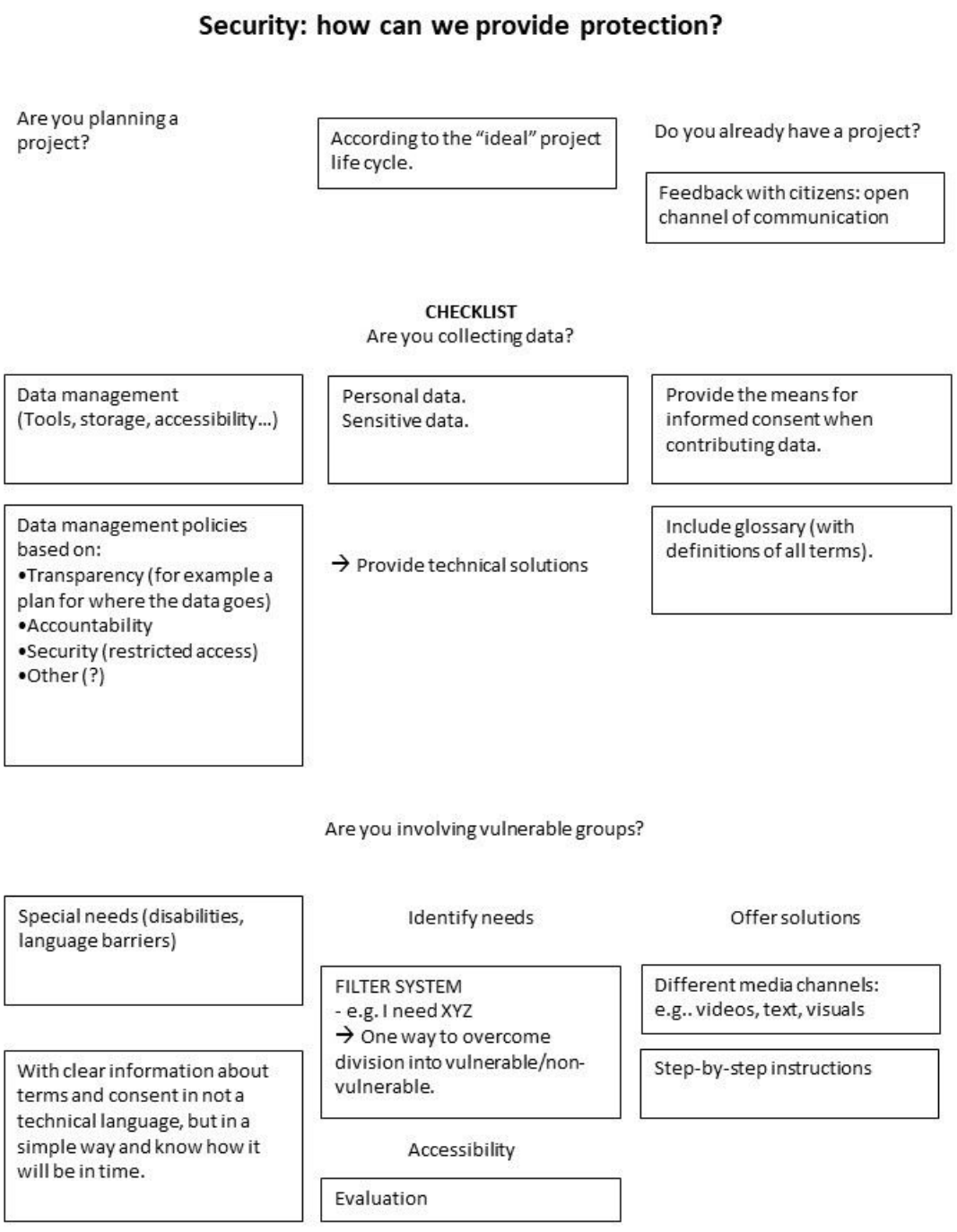


Figure 10. Group 2 mock-up of the citizens' information pack

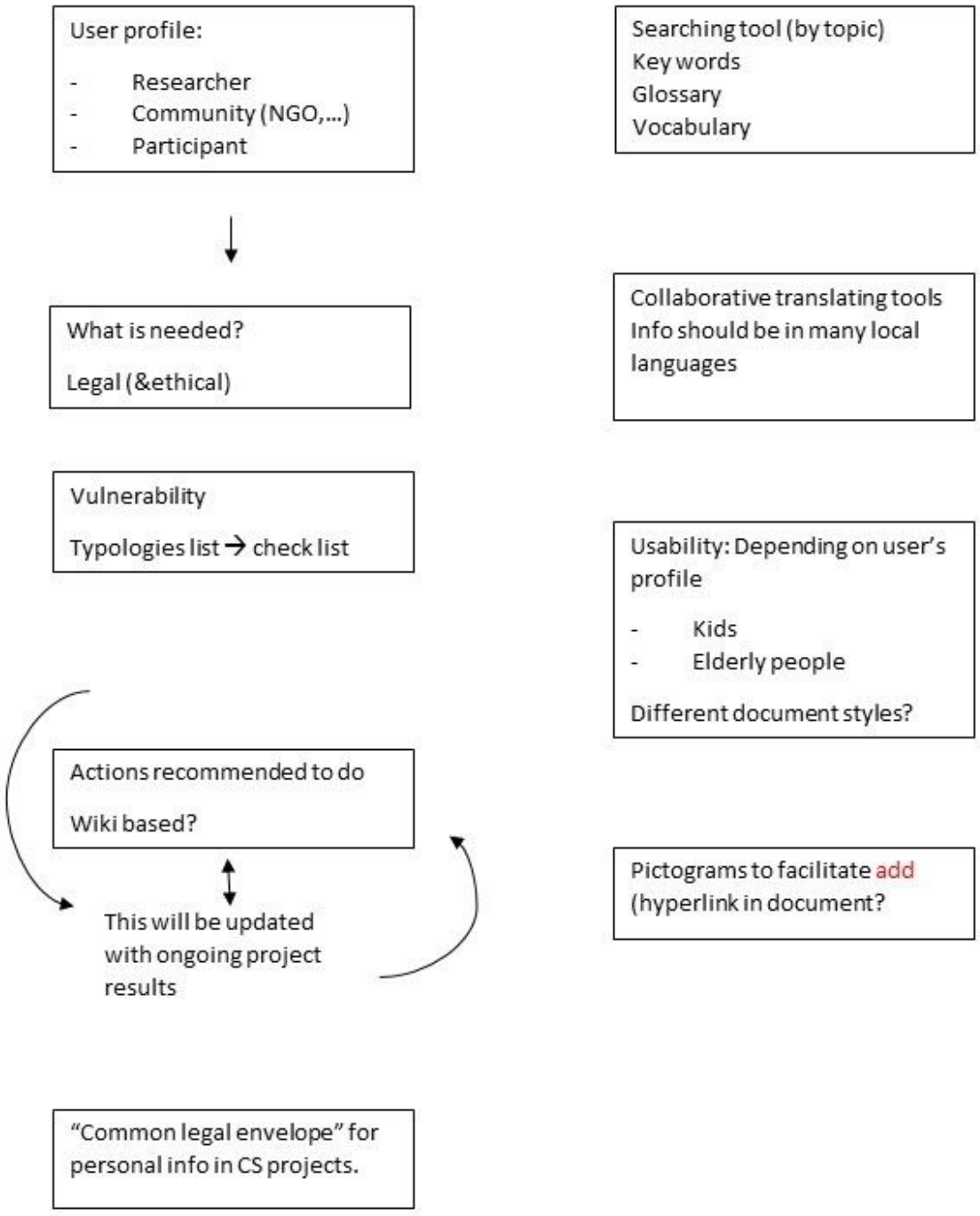


Figure 11. Group 3 mock-up of the citizens' information pack

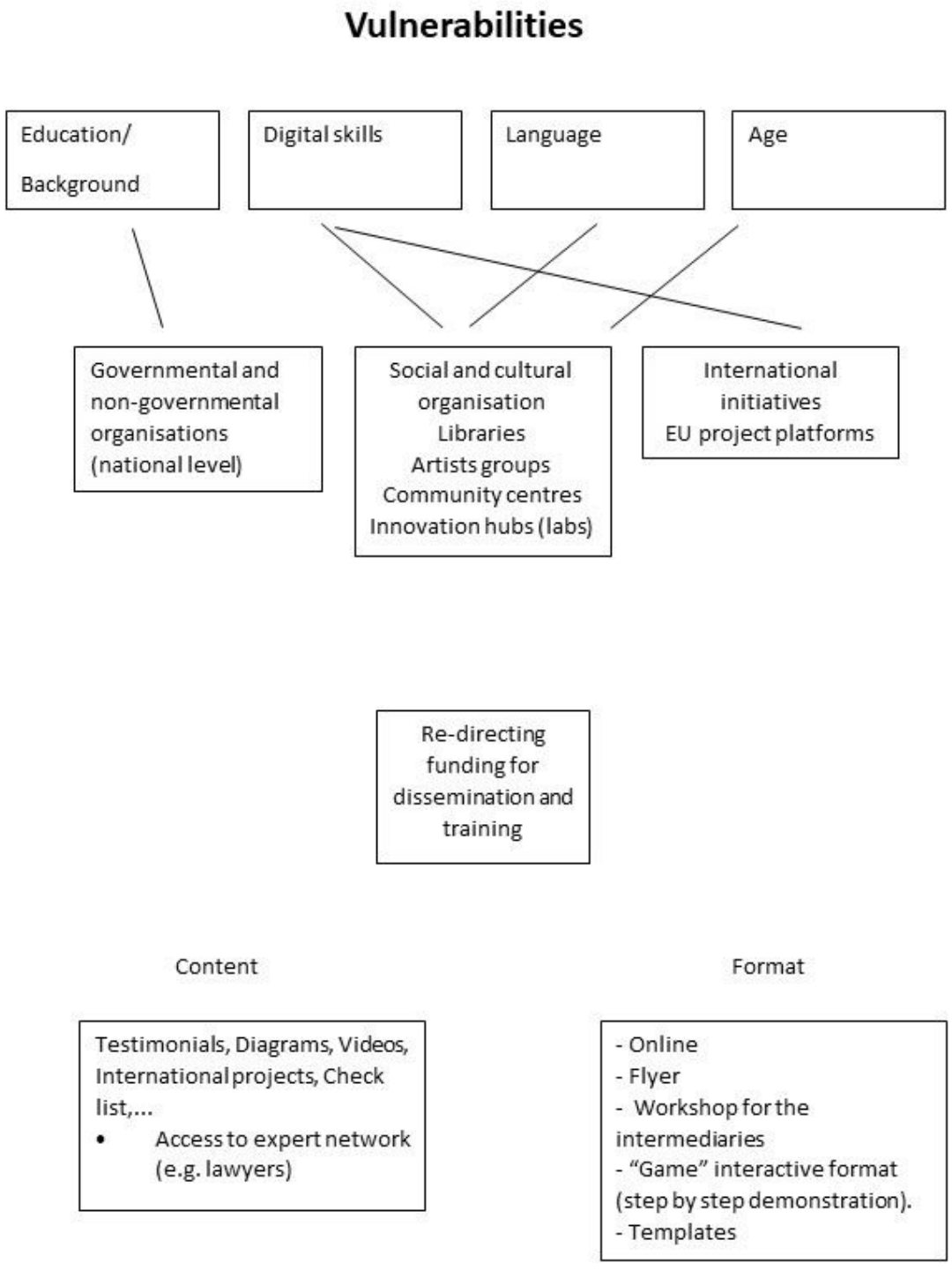
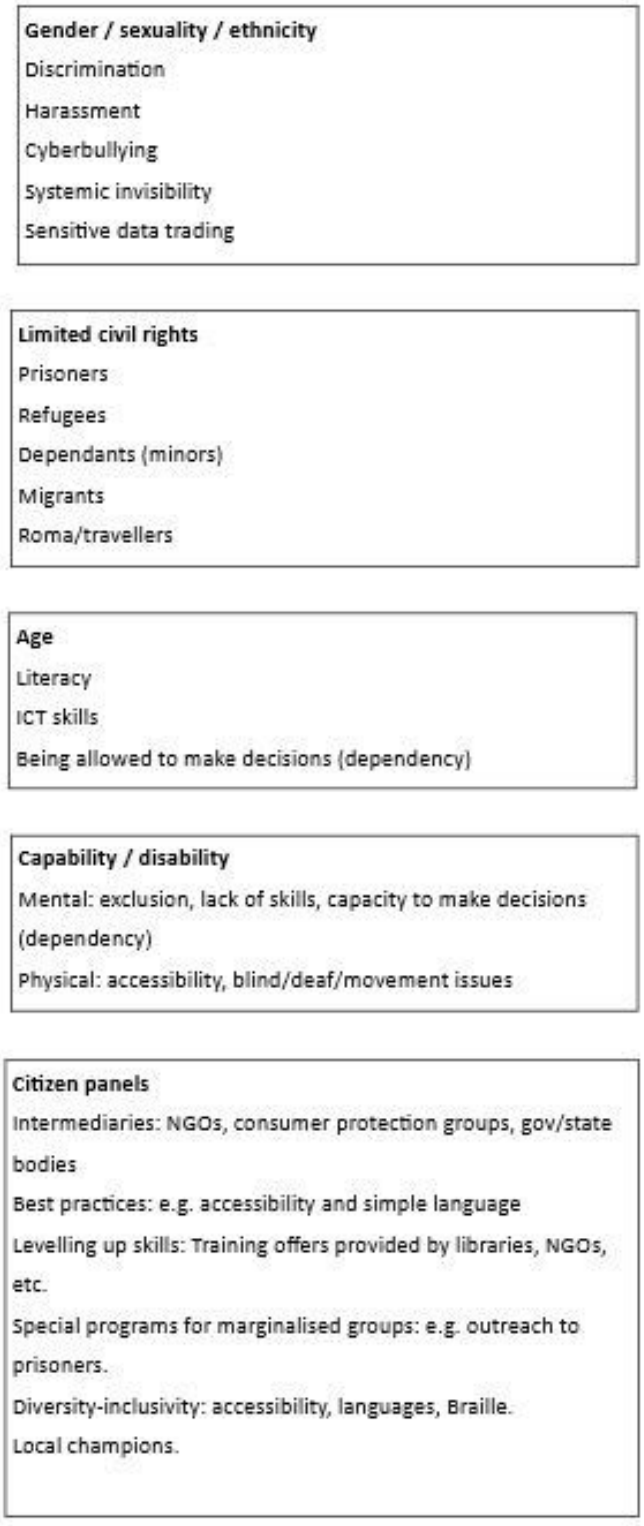


Figure 12. Group 4 mock-up of the citizens' information pack



Session 6 conclusion
These mock-ups provide a starting point for planning the final structure and content of the citizens' information pack. However, given the composition of the workshop participants, who were mostly from the fields of citizen science and/or academica, there is a need for further scoping to ensure citizens have a stake in this process, and that their needs and suggestions are considered when determining the final format. This will be an important next step for the PANELFIT project.
For the citizens' information pack tailored to vulnerable populations, it will be important to check the many sources of information (e.g. websites, institutions) that exist and consider whether it is sufficient for a certain vulnerable group to refer to these, or whether they need 'translating' into something that is better suited and more digestible.

Conclusions and next steps

This workshop provided an important step towards creating a citizens' information pack, and a version tailored to vulnerable people. It has progressed two essential processes for this work: (1) considering the best structure and necessary content for the information pack; and (2) mapping out who is vulnerable in Europe.

This second process is perhaps the trickier to complete. As this workshop highlighted, while there are several groups that can be classed as vulnerable, and many types of vulnerability, these are not clear, rigid categories. People do not fit into neat, binary categories of 'vulnerable' and 'not vulnerable'; rather, vulnerability is a fluid, dynamic concept, one that changes with a person's age, (changing) circumstances and through factors beyond their control. Vulnerability is also subjective: one person may feel, or class themselves, as vulnerable whereas someone else, in a similar (or perhaps even worse) situation may not.

Another way of considering this is to view vulnerability as a reflection of the diversity in society, and the relationships between different social groups. Diversity is often related to conflicts, disagreement, stereotypes and discrimination, which can be considered the causes of vulnerability. Thus, the citizens' information pack could be seen as a tool for diversity management, or diversity promotion.

As vulnerability varies widely within Europe's populations, so does people's vulnerability in relation to data rights and privacy. As Table A1 shows, this is not always simple to establish, or assign to particular groups. Some groups that share a type of vulnerability may have different data challenges (e.g. due to their differing contexts), while those with a certain vulnerability may find the data challenges they face shift over time, either improving (e.g. through new technology and laws) or worsening (e.g. as their vulnerability worsens). When looking for concrete solutions, it may be easier to consider the barriers that some

vulnerable groups face, and then explore further how each barrier can be lessened or overcome.

Lastly, there is a need within Europe for some form of 'data protection mainstreaming', similar in its aims to 'gender mainstreaming' or 'age mainstreaming'. In practice, this would ensure that data protection issues - including (and especially) those facing vulnerable groups - are considered in every activity in which data is sought, collected, stored or used. In this way, the citizens' information pack that PANELFIT will produce could be not only a reference document for those responsible for legal and ethical issues around ICTs, but also a 'soft' policy tool to encourage the wider consideration of these issues across Europe.

Next steps

For PANELFIT, the outcomes of this workshop will be used to start planning the citizens' information pack in more detail. A concurrent step will be to conduct a wider survey of the population about the ethical and legal issues around ICTs, and the challenges they face in this regard. As noted in this report, the views from the workshop participants cannot be considered as representative of all European citizens, being skewed heavily towards academics and those working in the field of citizen science. An online questionnaire or survey is a possible next step in this respect.

For ECSA, COST Action 15212 and EU-Citizen.Science, the workshop's outcomes should mark a step forward in ensuring that citizen science activities consider the needs of vulnerable groups, in terms of ICTs and data, but also in terms of ensuring the field is open to and inclusive of all groups and citizens in Europe. A follow-up action here will be to share the workshop outcomes (including this report) on the EU-Citizen.Science platform, and with ECSA's working group on empowerment, inclusiveness and equity. It will also be useful to look at existing definitions of vulnerability in the open data/open science literature and consider how well they apply within a citizen science context, and how they can be translated into understandable definitions for citizens.

References

Milan, S and Treré, T (2017) 'Big Data from the South: The beginning of a conversation we must have', *DataActive*, 16 OCTOBER, https://data-activism.net/2017/10/bigdatasur/

Suman, AB and Pierce, R (2018) 'Challenges for citizen science and the EU Open Science Agenda under the GDPR', *European Data Protection Law Review* 4(3): 284-295, https://doi.org/10.21552/edpl/2018/3/7

Annex 1. Participant list

Workshop participants		
Janice Asine	Open University	Jamaica
Corelia Baibarac-Duignan	Utrecht University	Romania
Elisabetta Broglio	Centre for Genomic Regulation	Spain
Alexandra Castañeda	Institute of Marine Sciences	Chile
Helen Feord	University of Edinburgh	France
Linda Freyburg	Museum für Naturkunde Berlin	Germany
Marcel Leppée	Institute for Healthy Ageing	Croatia
Andreas Matheus	Secure Dimension	Germany
Marta Camara Oliveira	Independent consultant	Portugal
Christoforos Pavlakis	Technical University of Crete	Greece
Jaume Peira	Institute of Marine Sciences	Spain
Karen Soacha	Institute of Marine Sciences	Colombia
Gefion Thuermer	King's College London	Germany / UK
Katrin Vohland	Museum für Naturkunde Berlin	Germany
Katherin Wagenknecht	Museum für Naturkunde Berlin	Germany
Tim Woods	European Citizen Science Association	Germany / UK
Katerina Zourou	Web2Learn	Greece
Online participants		
Federico Caruso	Osservatorio Balcani e Caucaso Transeuropa	Italy
Annelies Duerinckx	Scivil	Belgium
Andrzej Klimczuk	Warsaw School of Economics	Poland
Mieke Sterken	Scivil	Belgium
Anna Berti Suman	Tilburg Institute for Law, Technology, and Society	Netherlands

Annex 2. Workshop agenda

Monday, 9 March 2020

12:30-13:15 **Working lunch (vegetarian) and participant introductions**

13:30-14:00 **Session 1**: **Project introductions**

COST Action 15212, ECSA, Panelfit, EU-Citizen.Science, Cos4Cloud

14:00-14:30 **Session 2: Defining common language and definitions**

Personal data; data management; data use; data protection; security;

cybersecurity; GDPR; vulnerable people

14:30-15:00 **Session 3**: **What do we know about data protection and security?**

15:00-15:30 **Coffee break**

15:30-17:00 **Session 4**: **Mapping challenges and solutions**

- Personal and organizational challenges
- Summary based on the discussions held, to capture the main findings from the day
- Exercise for Day 2

17:00-17:15 **Wrap up of Day 1**

18:00 **Working dinner: who are Europe's vulnerable populations?**

Tuesday, 10 March 2020

09:30-10:30 **Session 5: Vulnerable populations in Europe**

A 'walkshop' around the museum, in small groups

- Who can be seen as 'vulnerable' in Europe? Building on discussions from previous evening
- How can we support their rights?
- What needs to be included in the citizens' information pack for these groups?

10:30-10:45 **Coffee break**

10:45-12:00 **Session 6**: **Prioritizing and designing solutions**

- Group work to create an initial structure and suggested content to feed to the PANELFIT editorial board

12:00-13:00 **Session 7: Working lunch (vegetarian)**

Wrap-up of main conclusions from the workshop

13:00 **End of the workshop**

Annex 3. Vulnerable groups identified within Europe

Vulnerable people and groups are more at risk of harm than others, and in many ways. This includes their data rights: their right to data privacy and protection. These data risks take many forms, but include (Niklas, 2019; Malgieri, 2020; PANELFIT consortium, 2020):

- power imbalances between data subjects and data controllers
- stigmatization, as people are put into groups
- data about them being open to misuse, and vulnerable people being less able to control or prevent this, because they have less power, knowledge or awareness
- vulnerable people being incapable of granting consent (in case of decisional vulnerability) or being harmed during the research project (e.g. due to physical or psychological frailty)
- these persons being harmed more than 'average' data subjects in cases where their data are transferred to other data controllers, for other purposes.

Some vulnerabilities are inherent, but for others, vulnerability can worsen or improve over their lifetime. For example, people may experience changing personal or financial circumstances, changing health conditions, or changing political climates (e.g. governments more or less supportive of marginalized groups). Furthermore, individuals in a group may be vulnerable in different ways, or experience different levels of the same vulnerability; not all elderly people are equally vulnerable, for example.

Indeed, the very nature of describing a certain type of vulnerability with one term may lead to ignoring the specificities within a range of conditions - which in turn risks overlooking or failing to address individuals' specific challenges.

A useful example here is people with impaired vision. Even during our workshop, participants identified 'blind people' as a group who are vulnerable. Yet for many people, blindness is not an 'all or nothing' condition: there are many vision-related disorders, which often worsen with age and/or disease and, for most people, are irreversible. In terms of data and rights, this may cause problems when it comes to reading information on small screens (e.g. smartphones).

Yet there are solutions to this, such as adjusting the contrast / font size of the screen, or text-reader services for fully blind people. The issue is that people need the solution that meets their needs. Trying to address this spectrum of vulnerability with one solution could lead to measures that still leave some within the category 'blind people' as vulnerable - even though the project or researcher has tried (and may think they have done so successfully) to address this.

Similarly, some people are vulnerable in specific contexts. For example, the Clinical Trial Data Regulation, which only refers to a specifically limited and delicate area of research, considers different categories of vulnerable individuals in research: frail, multiple chronicle conditions, mental disorders, older (Recital 15), incapacitated (Article 10(2)), pregnant or breastfeeding (Article 10(3)).[14]

It is clear that vulnerable people should receive greater attention in relation to ethical and legal discussions around ICTs, and be better included in development and deployment of ICTs and new technology (e.g. AI). These groups therefore need specific safeguards to be protected in terms of their data privacy and how data about them is used (Niklas, 2019).

However, there is currently no single definition of vulnerable data subjects in EU literature (Malgieri, 2020), which makes it difficult (maybe impossible) to create a definitive list of these groups. Nor is it necessarily desirable, due to the dynamic nature of vulnerability; as mentioned, a fixed list could lead to new or increasing vulnerabilities being overlooked.

Instead, Table A1 contains the groups and populations identified as vulnerable, as well as certain types of vulnerability.[15] As well as the groups identified during the workshop, it draws upon other sources in an attempt to bring together different strands of work around this subject.

Note that we have deliberately not attempted to sort these under headings or themes. To do so would go against one of the key conclusions of the workshop: that vulnerability should be something that is considered continually by project organizers, citizen science practitioners, researchers and all others responsible for managing the personal data of these groups. It should not be seen as a problem to be solved, or a box to be ticked; grouping types of vulnerability increases the risk of this happening. Furthermore, labelling groups as being vulnerable can reinforce their vulnerability and amplify discrimination and stigmatization (Malgieri, 2020). As far as is reasonably possible, no one should lose sight of the fact that these are people, above any other definition (e.g. data subjects, vulnerable groups, citizen scientists).

It is also important to note that this table is not an exhaustive list of all vulnerabilities, or of all potential vulnerabilities for each group, or their vulnerabilities with respect to data, ICTs and privacy. The examples given are to illustrate possible types of vulnerability for each group; many other types are likely to exist for each of these groups, depending on the degree of vulnerability and circumstances.

[14] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April, 2014, on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC (text with EEA relevance).

[15] For example, 'refugees' are a vulnerable group, but 'being poor' and 'being homeless' are a description of someone's state at a given time and in a given context.

Lastly, for some vulnerable groups identified, we have not identified a specific vulnerability for both categories (general; related to data, ICTs and privacy). This doesn't mean there is no such vulnerability, but rather that the contributors to this report have not identified one and did not want to overreach by assuming vulnerabilities for such groups.. This table should therefore be considered a 'living' table, that should be revised and adapted for future projects and publications.

Table A1. Vulnerable groups in Europe and the nature of their vulnerabilities

Vulnerable group	Possible nature of vulnerabilities	Vulnerability with respect to data, ICTs and privacy issues
Women	Pregnant or breastfeeding women may be or feel more vulnerable than other women.	
Single parents or guardians	Additional care duties may leave them with less time and resources to take care of themselves, increasing their vulnerability.	They may have less time and support to read about and understand these issues.
Parents or guardians of vulnerable children or dependants	Additional care duties may leave them with less time and resources to take care of themselves, increasing their vulnerability.	They may have less time and support to read about and understand these issues.
Homeless people	Multiple, including (but not limited to) greater health risks, increased risk of violence, unemployment and poverty.	Lower access to information about these issues. Also, data may be collected about them without their informed consent (e.g. when using homeless services, or by charities).
People with addictions (e.g. drug addicts, alcoholics)	Multiple, including (but not limited to) greater health risks, increased risk of violence, unemployment and poverty.	Reduced capacity to understand information about their rights with respect to these issues.
People suffering from, or at risk of, domestic violence and/or sexual abuse	Vulnerable to violence and psychological abuse, which is likely to have multiple impacts on their lives.	In some situations, victims' access to information may be restricted, due to the nature of the domestic abuse they suffer (e.g. a controlling partner who restricts what they can do).
Religious minorities	It can be difficult to erase bias away from these groups.	Some people may consider their religion to be a private matter, but certain unavoidable data-collection processes still require people to state this (e.g. tax regulations in Germany).
LGBTQ+ people and sexual minorities	Individuals in this group still face widespread discrimination across Europe.	New technology that violates privacy may be more likely to target such groups (e.g. facial profiling).

Transgender populations	Individuals in this group still face widespread discrimination across Europe. For example, Hungary recently passed a law ending legal recognition of trans status.[16]	Male/female tick boxes discriminate against them, while the 'traditional' language used in many situations (e.g. he/she, his/her) does likewise
Prisoners	Prisoners are cut off from their support networks, and often face additional threats (e.g. violence).	Being in prison may reduce access to information about their data and digital rights.
People leaving prison	Newly released prisoners may lack support networks, and find it hard to gain employment or secure housing.	Their vulnerable state may reduce access to information about their data and digital rights. Depending on how long they were in prison, they may be unaware of developments in terms of data protection and privacy.
People who are under-educated and/or poorly educated	Their vulnerability is exacerbated by not being aware of, or able to understand, support systems to reduce their vulnerabilities. They may tend to have lower incomes, increasing their financial vulnerability.	Information about ICTs, privacy and data rights tends to be complex and hard to understand; low education will increase this barrier.
People who are outside of training/education	This situation can exacerbate many types of vulnerability, including financial, health (especially mental health) and networks.	Information about rights can often be passed through these formal settings. Being outside of them reduces people's access to such information.
People who are misinformed, including those who may not be able to understand the information provided	Information is power; those who cannot access or understand information designed to help them are, as a consequence, more vulnerable than those who can.	This is true of digital information as well.
People with learning difficulties (e.g. dyslexia, dysorthography, dysgraphia, dyscalculia)	Learning difficulties can make people vulnerable in a multitude of ways; people who cannot understand information designed to help them are, as a consequence, more vulnerable than those who can.	These learning difficulties make it harder to find out about and/or understand information related to data rights, data privacy, ICTs, etc.
Indigenous groups	They may require the protection of their heritage (e.g. in museums).	We need to take into account provenience data (from provenance research on the

[16] See: www.theguardian.com/world/2020/may/19/hungary-votes-to-end-legal-recognition-of-trans-people

		origin, ownership and custody of objects) and people's knowledge, which may be stored without their knowledge or approval. There are risks concerning their traditional knowledge and how they understand their relationship with this issue (data protection and rights). What interests the researchers may not be what the group themselves need or want. Particular themes are often over-studied, while others are overlooked.
The Sámi (the only European people on the UN's list of Indigenous Peoples)	As a minority group, living in one of Europe's harshest regions, the Sámi experience many types of vulnerability. A report by the United Nations Special Rapporteur on the rights of indigenous peoples concluded that Sweden, Norway and Finland do not fulfil their stated objectives of guaranteeing the human rights of the Sámi people. [17]	The Sámi have always been a targeted group for different types of research. This includes register- and biobank-based research. These projects have sometimes bypassed ethical considerations, for example by failing to fully communicate that a project is targeting the Sámi people.
Ethnic minorities	Ethnic minorities in a country often face discrimination and may exhibit a higher prevalance of several types of vulnerability (e.g. low income, low education, health issues, language barriers).	They may have lower access to information about their data rights (e.g. due to language issues).
Refugees	Refugees often face discrimination and may exhibit a higher prevalance of several types of vulnerability (e.g. low income, low education, health issues, language barriers).	They may be reluctant to provide personal data due to concerns about misuse; this may exclude them from the potential benefits that ICTs can offer.
Asylum seekers	Migrants often face discrimination and may exhibit a higher prevalance of several types of vulnerability (e.g. low	They may be reluctant to provide personal data due to concerns about misuse; this may exclude them from the potential benefits

[17] See: www.iwgia.org/en/sapmi.html

	income, low education, health issues, language barriers).	that ICTs can offer.
Migrants	The nature of migrants' vulnerabilities varies widely. Economic migrants may experience many of the vulnerabilities that face refugees and asylum seekers, while high-income expats may experience very different vulnerabilities (e.g. stress, resentment among the local population).	Language may be an issue that increases the risk of their personal data being misused. Also, the data and ICT regulations in their new country may differ to those they are used to.
Members of traveller communities	Traveller communities often face discrimination and may find themselves outside of formal support networks (e.g. schools, healthcare, etc.)	They may be reluctant to provide personal data due to concerns about misuse; this may exclude them from the potential benefits that ICTs can offer.
Members of the Roma community	The Roma have been historically persecuted across Europe, which leaves many Romani more vulnerable than other populations, in terms of low income, employment, threats to their welfare, and many other forms of vulnerability.	They may be reluctant to provide personal data due to concerns about misuse; this may exclude them from the potential benefits that ICTs can offer.
Sick or injured people, including hospital patients and long-term patients	Health issues make people vulnerable in themselves, and can exacerbate other types of vulnerability (e.g. loss of income).	They may not be able to give consent to how their data is used. They may give consent too easily, for example if they want medical research to make them better (temporary vulnerability).
People with chronic/ long-term conditions, or multiple chronic conditions	Vulnerabilities are determined by the nature and severity of the condition. As an example, people with epilepsy may be vulnerable to exclusion from anything conducted online due to flashes/ light from screens (photosensitive epilepsy).[18]	These conditions may prevent people reading data privacy statements or consent forms.

[18] There are, however, free online tools that perform photosensitive epilepsy analysis; see, for example, www.w3.org/TR/WCAG20-TECHS/G15.html; Mozilla's website also has a section on accessibility solutions for developers (https://developer.mozilla.org/en-US/docs/Web/Accessibility/Seizure_disorders).

People with disabilities and disorders, either physical or mental (or both), and both temporary and permanent	Vulnerabilities are determined by the nature and severity of the disabilities and disorders. As an example, people with limited mobility may be dependent on others, increasing their vulnerability.	Some disabilities may mean people need assistance to access or share data, or to understand privacy statements / give consent. This reduces their control on their own data privacy.
People with limited communications capacity (e.g. speech impediments)	Limited communications capacity prevents people requesting, or contributing to, information in a range of scenarios. This may mean their needs, views or expectations are not considered.	Some limitations in communications capacity may mean people need assistance to access or share data, or to understand privacy statements / give consent. This reduces their control on their own data privacy.
Visually impaired / blind people	While many provisions exist for visually impaired and blind people, these may not be available or affordable for all people, increasing the vulnerability in many cases.	They are likely to use software that reads the screen / platform to them, which reduces the privacy of that information. Further, they might find their access to information restricted, for example if the websites to which they need access don't comply with the law and don't allow the software to read everything (e.g. options in tick boxes).
People excluded by language, or facing language barriers / networks (e.g. migrants, refugees, minorities such as Creole speakers in Portugal)	People who do not speak the language of their country of residence have reduced access to information about support measures, which increases their vulnerability.	Non-native speakers within a country, or minority language speakers, often lack information about their data and privacy rights in their own language.
People who are not fluent in English	As English is the predominant language across Europe, certain information may only be available, or more prominently available, in this language. Those who cannot speak or understand English may find themselves more vulnerable than those who can.	Much of the information on data rights and privacy is in English, putting these groups at a disadvantage.
Children / dependants / minors	Younger people are inherently vulnerable, lacking many of the attributes that reduce vulnerability (size, strength, completed education, independence, income, etc.)	Young people cannot legally consent to the use of their data. They may not know how to complain about misuse of their data, or be aware that they can or should.

Emerging adults (aged 20-30)	In many countries, this age group struggles to access the advantages that older generations did, such as secure, well-paid jobs, and housing.	A lack of employment and/or housing may make it harder to access information about digital rights and ICTs (e.g. due to the lack of internet access at home).
People aged 30-40	In many European countries (e.g. Portugal, Netherlands), this age group have a greater tendency to be self-employed or freelancers, and as such, especially during moments of crisis (such as the current COVID-19 pandemic) are vulnerable to dramatic changes in their income. They may also have young families, and hence have an increased level of vulnerability (e.g. financial).	Conversely, they may potentially have higher levels of technical skills and education than other age groups. This means they are less likely to be vulnerable to legal and ethical issues around data privacy, ICTs and their digital rights.
Older, frail or incapacitated people	Old age is another inherently vulnerable stage of life, as people may become weaker and more dependent on others.	While old age is not always linked to digital illiteracy, there may be lower awareness of legal and ethical issues around ICTs, data and privacy than among the 'digital generation' who have grown up with this technology.
People who are unemployed (or underemployed), both short term and long term	Unemployment exacerbates other forms of vulnerability, especially financial vulnerability and housing. It may also lead to health and mental health issues.	Unemployed people may lack the ICT training and information provided through places of work. They may have no online access at home (due to financial reasons), meaning they are unaware of information about ICTs, which is increasingly shared online.
People who have low economic status	Similar to unemployment, low economic status exacerbates other forms of vulnerability, especially financial vulnerability and housing. It may also lead to health and mental health issues.	People in this group may have no online access at home (due to financial reasons), meaning they are unaware of information about ICTs, which is increasingly shared online.
Social care clients and beneficiaries	People in social care may experience many other forms of vulnerability: poor health, low income, uncertain housing, etc.	People in this group may lack access to ICT training and information provided through places of work, and may have no online access at home (due to financial reasons), meaning they are unaware of information about ICTs, which is increasingly shared

		online.
People who are illiterate	Much of the information that governs our lives and aims to support us is provided primarily in written forms. Illiteracy is a major barrier to accessing this, leaving these people increasingly vulnerable. Illiteracy may also be linked to lower economic status.	A lot of information about legal and ethical issues around ICTs is shared in written form, especially online. Illiteracy means people will be less aware of, and less able to understand, this information.
People who are digitally illiterate / have limited technology expertise	Much of the information that governs our lives and aims to support us is increasingly provided online (e.g. doctor's appointments only bookable online, information that is only shared through social media).	These people are at risk of being left behind as information and services move increasingly online.
Offline communities	While not the same vulnerability as digital illiteracy (this is an access/infrastructure issue, rather than a skills or capacity issue), offline communities will face many of the same vulnerabilities as those who are digitally illiterate.	These people are at risk of being left behind as information and services move increasingly online.
Those with limited access to infrastructure	As an example, people in rural areas in some countries lack good access to infrastructure such as hospitals, libraries, strong broadband, childcare, and other support networks. This makes them relatively vulnerable, especially during crises (such as the ongoing COVID-19 pandemic).	Lack of infrastructure may extend to limited internet access (e.g. no or expensive broadband) and other ICT services. This can reduce people's access to information about their rights related to ICTs, data and privacy.
Research teams that are under-resourced		With limited time, money and (in some cases) information, they may be unable to implement the necessary measures to ensure the data and privacy rights of their subjects.
Communities who remain outside of the research process	Science and research underpins many elements of society (e.g. healthcare, governance, education). By being outside of these processes, either as researchers or subjects, these	This is true for ICT-based research as well: communities with no stake or voice in the process, or no access to the findings, may find that the impacts of such research (e.g. policy, funding decisions) do

	communities find their lives influenced by research in which they have no stake or voice - so solutions and research-led policies may not benefit them or reduce their particular vulnerabilities.	not address their needs or support them.
People hit by phenomena beyond their control, such as extreme climate events	Extreme events or phenomena can cause unexpected vulnerability. While this may take the form of natural events (e.g. floods, volcanoes, global pandemics), it can also be in the form of life events, such as unexpected illness, accidents, loss of employment, a death in the family, etc. The unexpected nature of such events makes it difficult to prepare for them, leaving people less resilient.	
Any citizen who, for any reason, considers themselves to be vulnerable	The nature and severity of this vulnerability depends on the perception of the subject. However, it is important to recognize that vulnerability is not a simple, measurable issue, but can be subjective, hidden and personal.	

Sources for Table A1

Workshop on 'Creating a citizens' information pack on ethical and legal issues around ICTs: what should be included?', 9-10 March 2020, Berlin.

Talk on 'Vulnerable populations' by Dr Jedrzej Niklas, Department of Media and Communications, LSE, UK (formerly University of Leeds), at the PANELFIT workshop, 5 June 2019, in Bilbao, Spain.

Personal communication with Professor Anna Lydia Svalastog, Department of Health and Social Studies, Østfold University College, Norway.

Personal communication with Professor Iñigo de Miguel Beriain, Department of Public Law University of the Basque Country.

PANELFIT consortium, 2020 'D5.2 Critical Analysis of the ICT Data Protection Regulatory Framework (Consolidated Version)', Bilbao, Spain.

PANELFIT podcast with Gianclaudio Malgieri, 'Vulnerable data subjects and EU Law', 27 February 2020 (available at www.youtube.com/watch?v=fqLfvF-cS70&feature=emb_title).