European Digital Public Spaces

Sander van der Waal, Marleen Stikker, Max Kortlander, Quirine van Eeden, Tom Demeyer, Stefano Bocconi

August 2020

waag
technology & society

Online European Public Spaces

Sander van der Waal, Marleen Stikker, Max Kortlander, Quirine van Eeden, Tom Demeyer, Stefano Bocconi

© Waag, august 2020
This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International license

Table of contents

Special Thanks

Towards a Digital Public Spaces movement

We would like to express our gratitude to the following people and organisations who we have spoken with in the course of this research. The clearer expression of the vision and mission that we define as primary outcomes of this work would not have been possible without their contributions. We look forward to inviting their commitment to this shared mission that we have distilled from these conversations and moving forward to implementing this mission together.

Name	Organisation or initiative
Sahar Yadegari	Adessium
Esra Kücük	Allianz Kulturstiftung
Aysu Arican	Anadolu Kültür
Nebojsa Glisić	B92 Foundation
Ian Forrester	BBC R&D
Johan Groenen	Code for NL
Carlotta Galuppo and Paola Sabbione	Compagnia di San Paolo
Annelie Berner	Copenhagen Institute of Interaction Design
Aik van Eemeren	CTO office, City of Amsterdam
Guillermo Peris	EDRi - European Digital rights coalition
Laura James	Enterpreneur in Residence, University of Cambridge
Menno Weijs	European Cultural Foundation
Lisa Bertel	FASresearch (Vienna)
Boris van Hoytema	Foundation for Public Code

Martijn de Waal	HvA (Amsterdam University of Applied Sciences)
Ruurd Priester	HvA (Amsterdam University of Applied Sciences)
Arash Aazami and Edwin Edelenbos	Internet of Energy initiative
Paul Keller	IVIR / Shared Digital Europe
Balázs Bodó	IVIR, University of Amsterdam
Ronald Huizer	Koninklijke Bibliotheek
Joe Doran	Lankelly Chase Foundation
Jasper Etten	Ma.ak020
Ruben Brave	Make Media Great Again
Marta Klepo	MitOst
Solana Larsen	Mozilla Foundation
Maria Exner	My Country Talks, Zeit Online
Teemu Ropponen	MyData
Paulien Dresscher	Nederlands FilmFestival
Johan Oomen	Nederlands Instituut voor Beeld en Geluid
Katja Bego	NESTA
Tim Franssen and Sergej van Middendorp	NUTS (https://nuts.nl/)
Sacha van Tongeren	Oba (Amsterdam public library)
Jan Hein Hoogstad	Offcourse
Ena Pervan and Ondrej Liska	Porticus Foundation
Leonie Thalmann	Pro Helvetia
Geert-Jan Bogaerts	PublicSpaces, VPRO
Melanie Rieback	Radical Open Security
Danny Lämmerhirt	Researcher

José van Dijck	Professor in media and digital society, University Utrecht
Stefania Milan	Associate Professor of New Media and Digital Culture, University of Amsterdam
Natalie Nougayrede	Robert Bosch fellow, Guardian
Victor Reijs	SIDN Labs
Douwe Schmidt	TaDa
Jakub Parusinski	The Fix, London, Kyiv
Jean F. Queralt	The IO Foundation
Georg Diez	The New Institute, Berlin
Iskander Smit	ThingsCon
Nadiia Kovalchuck	Ukrainian Cultural Foundation

Finally, we want thank our team at Waag: Job Spierings, Alain Otjens, Tessel Schouten, Sophie Almanza, Richard van ’t Hof en Thijs van Himbergen.

Summary

The Introduction identifies the need and opportunity to develop digital public spaces within Europe.

Chapter 1 defines the problem and concern of digital public spaces, and identifies foundational values for these spaces. Physical public spaces are compared with physical private spaces to identify certain qualities of each, and to gain an understanding of how public and private spaces may also take form digitally. This exploration demonstrates that most of our digital spaces are privately owned by companies. This context, coupled with the reality that many existing laws to protect human rights are not rigorously applied to digital spaces, poses a threat to democratic societies and points to the need to develop open digital public spaces where people have the right to act as citizens rather than consumers.

Europe is introduced as a viable context for developing such open digital public spaces. The Treaty on European Union provides a legal basis for considering these spaces. The European Commission also provides further recommendations for 'Shaping Europe's Digital Future'. These values are considered alongside other public values which we identified through interviews and research into existing digital rights initiatives in Europe.

Ultimately, we identify three values to build upon:

- **Open:** Digital public spaces need to be inclusive and accessible for everyone;
- **Democratic:** Digital processes are as transparent as possible; gatekeepers of information can be held accountable; citizens feel safe and in control over what happens with their personal data and citizens are empowered to act and to interact in these digital public spaces
- **Sustainable:** We build lasting and digital public spaces that are *socially* and *democratically* sustainable as well as *environmentally* sustainable.

In addition to the values themselves, we propose a set of **preliminary rules** to uphold them:

- Digital public spaces should be places of engagement which are equally available to everyone; which facilitate various metrics of locality; and where commercial initiatives find only a temporary foothold.
- Citizens ought to be free to interact with one another with the knowledge that they are not being tracked, interfered with, or manipulated by third parties.
- Digital public spaces ought to account for the more fair and even distribution of *scarcity* in online spaces – not scarcity of land and material resources as in physical spaces, but scarcity of findability and attention.
- Digital public spaces should have rules that are embedded in democratic structures and, where possible, should be enforced through the fabric of this environment, i.e. the protocols that govern the presence of participants and exchange of data and media.

Chapter 2 explores two use cases by applying the method of the public stack. These two cases, identity management and video conferencing tools, are respectively a building block or a key tool for building digital public spaces. The public stack in turn helps to envision the complexity that underlies technology as consisting of different layers, each with its own function. The relevant stack layers and dilemmas differ depending on the concept or tool that is subject to research.

In identity and authentication we see the need for a conscious consideration of its foundation (i.e. the values and rights it reflects), particularly through examining the notion of authenticity in the protocol layer. With regard to video conferencing, we consider the infrastructure that makes video conferencing possible, and elaborate on how different technological settings can impact the user experience and user rights such as privacy. Furthermore, we demonstrate the need to be aware of somewhat conflicting considerations that we see in many other technologies on different (peer-to-peer or client-server) configurations.

Chapter 3 reviews **current progress** towards creating digital public spaces and **identifies gaps** in this progress. **Current progress** includes:

- The identification of some components for designing and developing ethical technology
- Participatory approaches to research and design in technology and governance
- Some experimentation into inclusive data governance models
- Examples of technology that bring the some or all of the above assets together and are based on ethical principles and/or made in the public interest, and
- Enthusiasm – from citizens, developers, governments at all levels – to make a change and reimagine public space.

The **identified gaps** are:

- A shared vision and mission
- A shared foundation, 'set of values' and/or 'digital social contract' that can underpin the development of technology
- A clear and concerted effort to democratically bring these elements together into a feasible and inclusive movement
- A shared digital infrastructure that begins the process of developing online public spaces in a way that can be adopted and adapted locally while also being interoperable internationally.
- An active digital sphere where these efforts can come together and be presented.

Chapter 4 presents a new vision and a mission based on the identified values, the analysis on potential solutions and the gap analysis. Our vision is the realisation of open, democratic and sustainable digital public spaces. Our mission is to create open, democratic and sustainable public spaces by 2025, locally and in Europe. The steps towards this mission are proposed along three tracks: 1. The development and mobilisation of an inclusive movement, 2. The creation of key building blocks of a shared digital infrastructure and 3. the realisation of a digital public space on a local level (in Amsterdam). The tasks in all tracks will be conducted at the same time as they continuously demand iteration based on the findings from the other tracks. The activities corresponding with these tracks will be researched and specified in the coming months in order to, eventually, bring us as a step closer to our mission.

Introduction

The distinction between 'real life' and 'digital life' is fading. For many people, our work, relationships, entertainment, political discourse, and citizenship have expanded from physical spaces into digital spaces. Due to the covid pandemic, we are living through various levels of lockdown. **How do you reimagine the public space once it opens again?** The same one we had, or a different one? Preparing the world after lockdown gives us an opportunity to reposition citizenship and public space in debates about technology and society.

In the physical world, there are public spaces where people are protected by certain legal and human rights. The digital world, however, is largely private: political discourse, commerce, and private communications online take place in private spaces which are not bound by a social contract or democratic accountability mechanisms.

The result is an online environment that treats people as users and consumers rather than as citizens. This environment priorities economic growth and surveillance, treating people's identity, privacy, and personal information as commodities that are neither owned nor regulated by the people themselves.

This current digital reality is not inherent to technology. Instead, the status quo points to the need and opportunity to build digital public spaces. Digital public spaces would ensure the same rights and values that we hold dear in our physical spaces. These spaces would be protective of human rights, subject to democratic accountability, transparent, and commonly shared rather than privately owned.

Europe provides a useful starting point for developing such digital public spaces. The E.U. has a clear list of human rights; it has shown interest in developing safe and open technology; it has the need for a truly shared public space amongst its member citizens and countries; and it can provide an alternative approach to technology: one which is based on common public values rather than on market values or state values.

Our mission is to create digital public spaces by 2025, locally and in Europe, based on a shared foundation. To do so, we will explore a number of social and technical considerations for such a space; analyse two use cases under the lens of a public [technology] stack; identify the needs and gaps we face in the development of digital public spaces; and begin to build a local coalition to spearhead the development of digital public spaces locally which can be shared, scaled, and adapted throughout Europe.

1. Definition and values of public spaces

Digital public spaces

Physical public spaces

The concept of *digital public spaces* (or an *online European public space*[1]) is complex at first sight. We can gain clarification by considering digital public spaces in comparison with their analog, physical public spaces. Public space is a shared domain, governed by laws and regulations that are rooted in values agreed to in a social contract. These commonly held rules and boundaries guarantee certain liberties and limit certain types of activity. Generally, public spaces are thought of as being open and accessible – however, there are always limits to their openness and accessibility.

In addition to public spaces, much of our lives also take place in *private* spaces which operate under their own rules within the limits of the law or the social contract within which they operate. These various types of private spaces may be confused with public spaces because they share certain similar qualities – they may be free, shared, or generally accessible. To add clarity, we can consider various types of public and private spaces which have nuanced (and sometimes overlapping or blurry) differences regarding openness, ownership, and rights:

1) **public spaces**, where people generally have a right to be and in which people are subject to certain rules based on the social contract and the context of that space. Examples include parks, city squares, public roads, and public schools;
2) **governmental-private spaces** where resources are shared by the public but are not openly accessible to the public. Examples include prisons, municipal facilities, and military areas;
3) **personal-private spaces**, which individuals have ownership over and where they can exercise their own rights and decisions as they wish within the limits of the law. Home is an example of a personal-private space;
4) **communal-private spaces**, which are open and accessible to a specific community which shares ownership, but where not access is not guaranteed for the general public. Examples include churches, community organisations, and allotments;
5) **corporate-private spaces**, which the owner (an individual or group) can 'manage as they please, to the exclusion of others'[2] and where the space is managed as a productive asset (rather than managed as a personal good, as is the case with personal-private spaces). Examples include stores and warehouses.

*In each of these senses, space is not purely physical, but might also refer to radio frequencies or access to other non-material resources.

[1] This report was originally titled 'Online European Public Spaces. The abbreviation of Online European public spaces, OEPS, has the unfortunate connotation of these spaces being 'accidentally' created where this is a deliberate choice. We use 'digital' instead of online as this is a broader, overarching term. From now on we will use the term digital public spaces.

[2] https://plato.stanford.edu/entries/property/

These definitions are not fully comprehensive. Rather, they intend to shed light on how space may be considered both online and offline, demonstrate how these types of spaces overlap and interact with one another, and help us to consider the nuanced limitations of public space and the ways in which public spaces are infringed upon or mistaken for other types of 'non-public' spaces.

Digital public spaces

These various types of spaces also exist in the digital world. Websites, the hardware we use, our apps, and fiber optics infrastructures can all be viewed as spaces. Considered in the terms above, there are numerous digital examples of these types of spaces:

1) **governmental-private spaces** exist online for example in the form of official government web portals, such as where you file your tax returns;
2) **personal-private spaces** are those digital spaces that are your property, such as a private server, CD players and the CDs you play on them, or a personal website you host yourself);
3) **communal-private spaces** are digital spaces that groups of people or organisations govern together; examples include cooperative online community platforms such as Gebied Online[3]; and
4) **corporate-private spaces** constitute the majority of the digital spaces we deal with on a daily basis; for example Facebook, or the operating system on your smartphone).are operating in a market context where you are a consumer.

A summary of this comparison between physical and digital spaces is portrayed in the table.

	Physical	Digital
Open Public Spaces	Parks, city squares, public roads, public schools (*note that each has its own limits to openness and accessibility)	
Governmental-private space	Prisons, municipal facilities, military areas	Governmental websites (tax filing, DigID); official platforms for reaching government, signing petitions, holding debate); surveillance infrastructures
Personal-private space	Home	Private server; self-hosted personal website; CD playlist
Communal/Common-private space	Churches, community, organisations, allotments	GebiedOnline, Decidim, YourPriorities, Polis
Corporate-private space	Store, warehouse	Facebook; Spotify playlist; Gmail; YouTube;

[3] https://gebiedonline.nl

The problem

But what about digital public spaces?

There are none.

While physical public spaces are upheld by a social contract, there is no such social contract which provides the foundation for designing, building, managing, and protecting public values in our shared digital spaces.

There is, of course, nuance to this argument. Some spaces do indeed come close to resembling digital public spaces, like certain online government portals, open forums, and publicly-funded tech. But there are various ways in which these spaces fall short of being truly open digital public spaces: the lack of applied and foundational public values with regard to tech; the private infrastructures which permeate various other spaces often without knowledge or consent of citizens; and many other issues which we will explore in the following chapters.

Since many services, and especially social platforms, offer their services free of any direct charge, they are easily and erroneously seen as forming a digital public space (a narrative which is central to their business model). In actuality, these companies offer a service or product from the context of a strictly private space where the rules are theirs – not subject to social or democratic accountability. On Facebook, for example, you do not have a right to free speech but rather are a consumer of a commercial platform and bound to the rules it sets for you. Still, users of commercial platforms like Facebook and Twitter argue that rights such as freedom of speech ought to apply. This friction plays out when, for example, a platform marks a post as 'fake news', bans a user, or utilizes black-boxed algorithms to manage what users do or do not see.

On the other hand, there are certain rules which do currently govern digital spaces. In theory, digital private spaces are required to operate within the laws of the physical space within which they are owned and operated or within which they are used (such as non-European technology that is required to comply with GDPR for European users).

In reality, however, many of the rights and values that we hold dear in the physical world have not been applied with any guarantee in the digital world. This can be seen in repeated challenges of human rights on European territory such as the protection of personal data, the right to respect for private life and the right to respect for family life.[4]

Online, our common guarantees to liberty are under pressure and fall short; our jointly-held rules and regulations do not effectively ensure those liberties and we ultimately see a breakdown of expectations for civility, privacy, ownership, and other values which we protect in the physical world.

[4] https://www.rathenau.nl/sites/default/files/2018-02/Human%20Rights%20in%20the%20Robot%20Age-Rathenau%20Instituut-2017.pdf

Moreover, there is an increasing trend of corporate private digital spaces entering into spaces which were previously personal private spaces or digital public spaces: IoT devices which store, analyse, and sell data regarding a person's home activities; political discourse which is owned by Facebook, curated and moderated (or not) by its employees and algorithms; a DigID account accessed through a Google browser which tracks the person's online activity.

The point is that we are losing public space as our lives become increasingly digital. All of this poses a threat: where can privacy, democratic debate, and shared spaces where human rights are upheld actually be found in a world which operates increasingly under rules set (and often concealed) by private corporations?

The Opportunity

We need to implement and enforce public values and rights which protect sovereignty, personal data ownership, and privacy in online spaces to ensure these principles both online and in our physical lives. These values and rights can form the basis for digital public spaces where people are citizens rather than consumers.

Citizenship in the digital era requires a digital environment based on public values, human rights, and shared principles for governance. But whose values, rights, and principles are these? How can we identify them? What are they? And how can they be technically embedded into digital spaces?

European values

It is helpful to define an area of focus to practically consider (and ultimately design, build, manage and protect) technology in relation to values, rights, and principles. For the purposes of this discussion, we will take Europe as a starting point.

A number of qualities make the European Union an ideal area to develop digital public spaces: it could allow for local development, testing and modification of digital public spaces while maintaining interoperability among member cities, regions, and states; European laws protect certain human rights already in both physical and digital domains; and European citizens and governments alike have expressed the need and desire to further protect European public values and rights in the digital era.

Europeans could benefit from having more shared European spaces. But what does it mean for a digital space to be European? We will draw from multiple sources and perspectives (but not rely on any one completely) to explore this question.

Positioning European Technology

Questions for society are questions for technology, and vice versa. Each digital protocol forces certain behaviours upon people, and thus has certain implications for the relationship between citizen, state, and markets. Protocols fit a certain narrative and are always based on values (whether explicitly or not). Much of the current technology we encounter is built open *free market economic* values (U.S.), *state power* values (China), and/or *surveillance and security* values (U.S. and China). The narrative of how individuals, communities, countries, organisations should relate to each other – one which prioritises citizens – is missing.

The narrative of *what protocols we need* and *what society we want* need to come together. We must bring the digital and physical in sync with each other once again. **We need to regain the sovereignty we have already lost, and defend and uphold our values in an increasingly digital world.**

What can Europe offer in this sphere? What do we want? How do we get there? A number of European initiatives (both governmental and independent) have begun to address these questions.

The European Union's Laws and Values for technology

Laws

In Europe, we already have a set of laws based on public values that intend to protect the rights and livelihoods of the inhabitants of the EU – most broadly, the founding principles of the EU[5]:

- Human dignity
- Freedom
- Democracy
- Equality
- The rule of law and respect for human rights, including the rights of persons belonging to minorities

Article 2 of the Treaty on European Union provides a legal basis for protecting these values in our digital spaces to the same extent as in our physical spaces.

Values

This sentiment is shared by the European Commission, who states in the new strategy 'Shaping Europe's Digital Future' that technology needs to be rooted in existing European values[6]: 'European values and ethical rules and social and environmental norms must apply also in the digital space' (p. 6). The strategy adds further specificity to the EC's official approach to technology by laying out three key objectives:

1. Technology that works for the people
2. A fair and competitive digital economy
3. Open, democratic, and sustainable society

[5] https://www.europarl.europa.eu/factsheets/en/sheet/165/human-rights

[6] https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

With regard to the 3rd objective of an **open, democratic, and sustainable society**, the strategy states that the EU's digital strategy will:

- use technology to help Europe become climate-neutral by 2050
- reduce the digital sector's carbon emissions
- empower citizens with better control and protection of their data
- create a European health data space to foster targeted research, diagnosis and treatment
- fight disinformation online and foster diverse and reliable media content

Finally, the strategy also explicitly states how the EC views its role in technology on the global stage, stating that the European Union will:

- aim to become a global role model for the digital economy
- support developing economies in going digital
- develop digital standards and promote them internationally

Building Upon Existing Laws and Values

Existing values – and the laws which enshrine these values as rights – can provide a solid social and legal basis for protecting rights in digital spaces. But in order to be truly comprehensive, these **existing laws which protect human rights need to be updated** to address the current digital reality.

The Rathenau Institute in the Netherlands researched for the Parliamentary Assembly of the Council of Europe (PACE) the impact of new technologies on human rights. The research considered technological case studies in relation to existing human rights such as the right to respect private life, human dignity, ownership, safety and liability, freedom of expression, prohibition of discrimination, acces to justice and the right to a fair trial. The report concludes that our understanding of how to protect human rights in the digital context is significantly underdeveloped and that the protection and further development of the current human rights framework is crucial for the robot age. The authors thus **advocate for new rights** including the **right to meaningful human contact** and the **right not to be measured, analysed or coached**[7].

The values of the European Union are just one lens through which to view the full spectrum of 'European values'. Indeed, it is not possible for a single individual or group to present public values in a top-down manner. The term *public values* implies that the values underlying digital public spaces must be identified and agreed upon as part of an open, collaborative, and long-term process which is beyond the scope of this research.

Nonetheless, we can start to understand what European public values for an online public space ought to be by asking people for their opinions, researching scholarship and initiatives which advocate for public values for technology, and drawing from those values, laws, and rights which have already been stated by the European Union.

[7] Van Est, R. & J.B.A. Gerritsen, with the assistance of L. Kool, *Human rights in the robot age: Challenges arising from the use of robotics, artificial intelligence, and virtual and augmented reality – Expert report written for the Committee on Culture, Science, Education and Media of the Parliamentary Assembly of the Council of Europe (PACE)*, The Hague: Rathenau Instituut 2017

Interviews and Research

Our research into values, use cases, and communities was guided by a series of interviews, group discussions, and conversations with people from across Europe who work in a number of fields related to society, digitalisation, and public space. These interviews were supplemented by previous co-creative research conducted by Waag to identify key values for technology held by citizens and public administrators.[8]

A common thread in what people communicated to us were their values in terms of needs, or what the *status quo* is lacking. These needs include:

- the need for a shared European space, particularly one which fosters dialogue and reinforces networks (values-based, grassroots) between Europeans
- the need for a place for human spaces online that prioritize and facilitate human-to-human interaction and collaboration
- the need for society to govern their own public spaces both online and offline, and the need for a commons through which to do so
- the need for human rights to be fully protected in digital spaces, such as safety, privacy, and the right to free speech
- the need for European alternatives for the tools that we use on a daily basis but which contradict our individual and shared values and
- the need for a European model which serves the public space and is based on European values that addresses private ownership, state surveillance, and democracy.

The unifying factor behind each of these values is that an online European public space is that it shoube based on public values. At first sight, this sentence may appear redundant. But indeed, a **public values-based approach** is what can distinguish European technology, and is precisely what is currently lacking in current dominant technological paradigms.

Existing public values for technology

Existing independent coalitions, initiatives, projects, and other groups within Europe (and globally) have developed or co-created sets of public values for technology, including:

- **Tada**[9]: 'Professionals from the Amsterdam region...wrote a manifesto entitled 'Tada – data disclosed'. Government authorities, companies and other organisations from different regions are invited to use and sign the document, showcasing their ambitions to shape a responsible digital city.'
- **Cities for Digital Rights**[10]: The 'Cities Coalition for Digital Rights aims to protect and uphold human rights on the internet at the local and global level.'

[8] A deeper explanation of the methodology is available in the Appendix

[9] https://tada.city/en/home-en/

[10] https://citiesfordigitalrights.org/

- **PublicSpaces**[11]: PublicSpaces has the mission to '[reclaim] the internet as a force for the common good and [advocate] a new internet that strengthens the public domain.' The values core to their mission have been defined as: open, transparent, accountable, sovereign, and user centric.
- **Mozilla Manifesto**[12]: Mozilla, perhaps best known for its Firefox web browser, has the stated mission to 'keep the internet open and accessible to all.'
- **Shared Digital Europe**[13]: 'This document summarises the efforts undertaken by Kennisland, Centrum Cyfrowe and Commons Network to develop a new vision for digital policymaking in Europe. To this end, [the authors] have created a new policy frame, in an effort to find solutions for a number of problems that plague the Internet.' Relevant to OEPS, the vision statement says, "Europe needs to establish its own digital space that embodies our values: strong public institutions, democratic governance, sovereignty of communities and people, diversity of European cultures, and equality and justice. A space that is common to all of us, but at the same time diverse and decentralised."
- **Open Data Institute (ODI)**[14]: ODI 'envisions a future where people, organisations and communities use data to make better decisions, more quickly...To bring about this future, we must make data as open as possible while protecting people's privacy, commercial confidentiality and national security.'
- **Amnesty International's 'Artificial Intelligence and Human Rights'**[15]: The Dutch chapter of Amnesty notes that: 'Because many systems are not transparent or have been developed with the wrong vision, they can make decisions that have major consequences for our private life. Violating our privacy is a major risk.'

[11] https://publicspaces.net

[12] https://www.mozilla.org/en-GB/about/manifesto/

[13] https://shared-digital.eu/vision/

[14] https://theodi.org/about-the-odi/our-vision-and-manifesto/

[15] https://www.amnesty.nl/wat-we-doen/tech-en-mensenrechten

The stated values and principles of each of the aforementioned initiatives can be found in further detail in Appendix 2. The image below indicates key words found throughout these sources[16]:

Outcome of research into values

In conclusion, we see that the European Union's fundamental values are still reflected in today's strategy on 'Shaping Europe's Digital Future'. At the same time, our interviews and research demonstrate that many organisations and people express a collective need for digital public spaces to be based on public values. 'Public values' generally refer to ideas that citizens are able to access these spaces equally, to have an equal say, that these spaces have accountability mechanisms, safeguard human rights and democratic institutions and so forth. This idea of public spaces in a European context is affirmed when comparing these ideas to other types of narratives on technology such as in the USA or China.

One of the three key objectives in 'Shaping Europe's Digital Future' contains a mission to create an **open, democratic and sustainable** society. We propose these as core values to build upon because they cover and include many of the other public values which have been identified; they are clear, concise, and comprehensive; and they provide an established route for approaching the development of digital public spaces in an officially European capacity:

- **Open**: Digital public spaces need to be inclusive and accessible for everyone
- **Democratic**: Digital processes are as transparent as possible; gatekeepers of information can be held accountable; citizens feel safe and in control over what happens with their personal data and that citizens are empowered to act and to interact in these digital public spaces
- **Sustainable**: We build lasting and digital public spaces that are socially and democratically sustainable as well as *environmentally* sustainable. Models such as Kate Raworth's 'Doughnut of planetary boundaries and social boundaries' are reflective of this multi-faceted approach to sustainability.[17]

[16] The text in this 'word cloud' was edited from the original reference texts to only include key thematic terms. This text (derived from the sources referenced in this section) is available for review in Appendix 2.

[17] https://www.kateraworth.com/doughnut/

In addition to the values themselves, we propose a set of preliminary rules to uphold them:

- Digital public spaces should be places of engagement which are equally available to everyone; which facilitate various metrics of locality; and where commercial initiatives find only a temporary foothold.
- Citizens ought to be free to interact with one another with the knowledge that they are not being tracked, interfered with, or manipulated by third parties.
- Digital public spaces ought to account for the more fair and even distribution of scarcity in online spaces – not scarcity of land and material resources as in physical spaces, but scarcity of findability and attention.
- Digital public spaces should have rules that are embedded in democratic structures and, where possible, should be enforced through the fabric of this environment, i.e. the protocols that govern the presence of participants and exchange of data and media.

This list of core values and preliminary rules is based on our review of research and interviews. Public values derived from this list may vary and their relative importance may change over time. It is important to continue to refine these values at a later stage, particularly as a project evolves. Further collaboration with governments, relevant organisations, and citizens is needed to co-develop a truly shared set of values for digital public spaces. Part of this collaboration will involve identifying ways to improve the application of existing laws, as well as developing and advocating for the addition of new rights for a digital age.

As this section demonstrates, many rights, values, and laws exist but are not widely applied. Much of the technology we use is developed under a contradictory set of values, only to have our current laws and values haphazardly and inconsistently applied once a problem is discovered. **What is needed, then, are not new sets of values, but rather something more reflective of a social contract: a new foundation to instill values in technology throughout the design and development processes.**

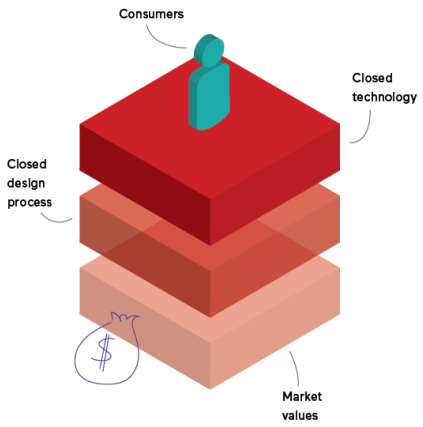
2. Public Stack and Case studies

- Chapter 1 provided an overview of public values that a digital public spaces could draw from, and argued for an outcome in which these public values form the foundation for new technological development.
- What would a new 'foundation' look like in technical and social terms? In Chapter 2 we present an exploration of two use cases (video conferencing and identity in social media) to get a better sense of what digital public spaces could be in terms of technology, design, and public values.
- The case studies are examined in the context of the 'public stack' framework, which considers technological layers within the broader context of societal, design, and citizen layers.

Different stacks

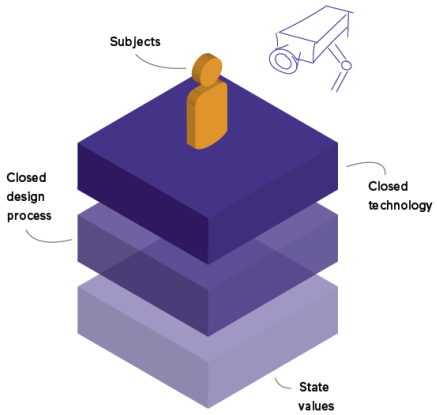
A full exploration of stacks and the public stack is available at https://waag.org/en/article/roadmap-digital-future. Below, a summary is presented to give context to the subsequent case studies, which are considered under this model.

It helps to envision the complexity that underlies technology as consisting of different layers, each with its own function. We call these layers a stack. **The stack of any given technological object or service is the entire range of components that make that object or service what it is.** Whether these are actual, physical components such as a phone's hardware and infrastructure, virtual components such as the apps installed and the data we produce, or conceptual components such as the business model or the data policy of the producer, they are all part of the stack, and they all determine how citizens use technology, and how technology uses citizens. Problematically, the 'stack' that we use today is largely the 'private stack' – its constituent parts have been developed by mostly private companies, and the stack is thus tailored to ensuring profit for those companies.



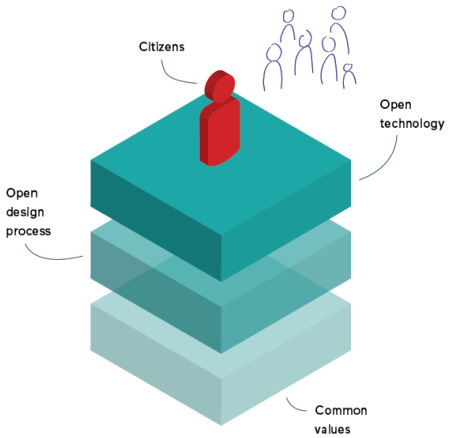
PRIVATE STACK

Some technologies are developed by decree of a government, and used to service and understand its citizens. These technologies are the result of a state stack, which often overlaps and interacts with the private stack. There are seemingly harmless examples in the state stack, such as online tax services. But there are also countries who make domestic and international surveillance central features of their 'state stack', using the large amounts of data that these technologies produce to analyse, influence and even police behaviour at the expense of privacy, sovereignty, and democratic values.



STATE STACK

It is important to look at the stacks under the surface of the technologies we use and wonder: do we agree with what happens there? Based on the values identified in Chapter 1, we do not. This is why we need **a public stack: a shared digital infrastructure to develop and connect technology, which puts public values at the center of the design process.**

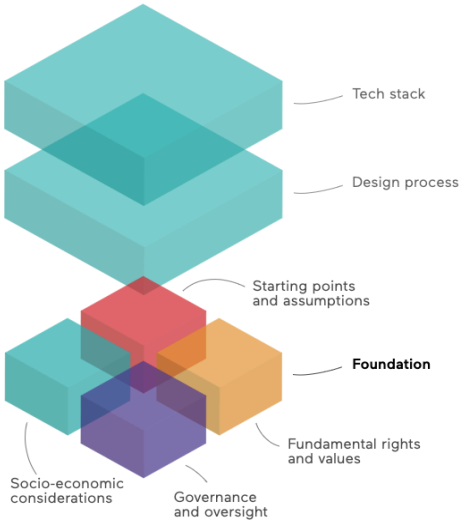


PUBLIC STACK

The Public Stack

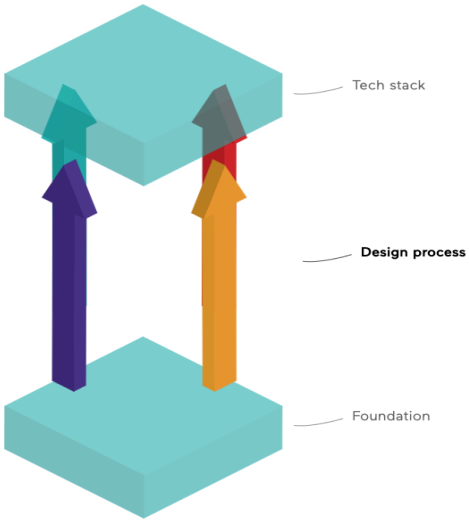
We envision the public stack to consist of four layers: the foundation, the design process, the technology and the citizen perspective as shown in the image in the previous paragraph. A more extensive description can be found below.

1. The *foundation* consists of the specification of assumptions and objectives of owners and investors; the way the law and societal values are taken into account; the way governance and supervision are organised; and the extent to which social and socio-economic considerations have been addressed.



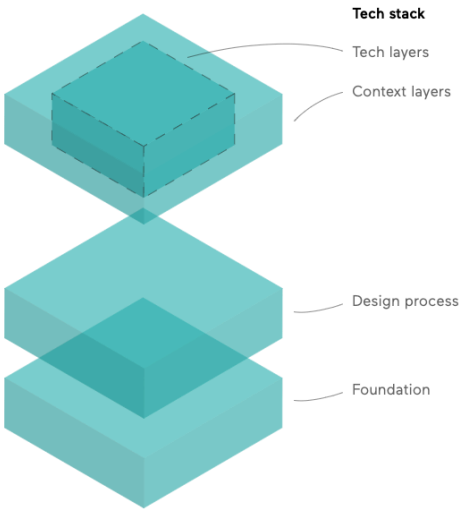
FOUNDATION

2. The *design process* specifies how the questions addressed in the foundation is reflected in the design (and development) processes for the technology stack.



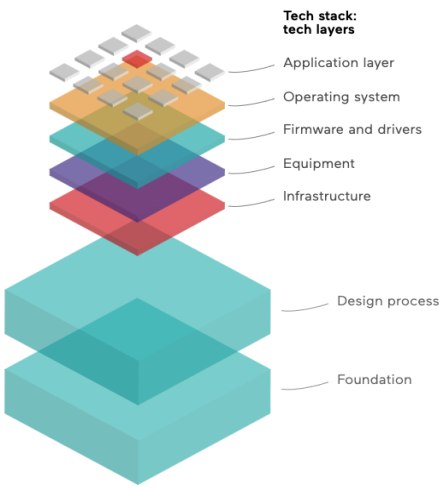
DESIGN PROCESS

3. The *technology stack* represents the structure of technology (i.e. Infrastructure and operating systems). These layers are then again connecting to each other by the 'context layers'. These context layers are constantly cooperating and communicating with each other.

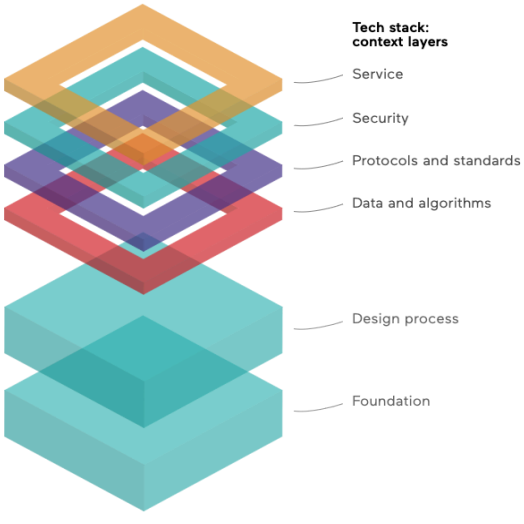


TECH STACK

An everyday example of the way the technology stack operates is by listening to a song via Spotify. The Spotify app on your phone has access to your headphones via the operating system and firmware so you can hear the song. The song itself is often streamed from a data center over the Internet infrastructure. There is a connection between each of the context layers which allow them to interoperate as parts of this technology stack.



TECH LAYERS



CONTENT LAYERS

4. The *citizen perspective* specifies how citizens deal with digitalisation and technology and the extent to which citizens have been involved in the design process

The public stack initiates a design with all stakeholders, based on a foundation of public values in which people and planet are taken into account and governance and supervision are set up in line with these values. Once all layers (as mentioned above) of an application/architecture reflect shared values and public participation, we could speak of an application in line with the principles of the public stack.

At the time of writing a preview of the public stack website is available on http://publicstack.net:8080/

Case Studies

The public stack is a model to unravel the decisions and values that are embedded within technology and their effects on people and societies. The public stack also helps to establish clear, ethical guidelines for new, alternative technologies within the context of digital public spaces.

In this chapter we use the public stack model to unravel the layers used in identity management and in video conferencing tools and propose a set of guidelines for both. We focus on the technological stack of both types of applications and distinguish between different layers within the technology. The complete case studies on identity management and video conferencing are available in full in the Appendix.

Identity management is a key building block for digital public spaces, most simply because if a system has regulations, then people are subject to those regulations and must be addressable. This is where issues of identity management come into play, which can lead to fundamental questions about who defines and manages identity and under which conditions. Our case study of identity management takes a human-centered approach to this subject in order to shed light on the nuanced implications that various technological options have for self, identity, privacy, and ownership.

Technical approaches to identity and authentication require a conscious consideration of their foundation (i.e. its values and rights), which becomes clear when examining the notion of *authenticity* in the protocol layer. The interplay between values, infrastructure, protocols and services is, from a civic perspective, one that needs careful governance, design, and monitoring as it has repercussions in terms of accessibility and participation, as well as the potential for detrimental social consequences, as we have seen in the discussion on reputation.

Video conferencing would be a key tool for people interacting in digital public spaces. It is a practical application of technology that is increasingly central to our lives, particularly during times of isolation and lockdown. It is also a sensitive technology by nature as it captures and transmits video and audio. Our case study into video conferencing takes a strong technological perspective to explore how various technical decisions, based on different sets of values, impact a person's safety and privacy. The case study considers which options are available in the present, and considers what is needed for video conferencing in public spaces.

Using the public stack layers we explain the infrastructure that makes video conferencing possible, and how different technological settings reflect on the user experience and user rights such as privacy. In a peer-to-peer configuration we can have more control and options to address important values such as privacy, while a client-server configuration feature richness and ease of use might be easier to achieve, but control and privacy might suffer, especially if the server is managed by an organisation we cannot trust. A possible compromise is to use a client-server solution run by an organisation we trust.

For both case studies, the public stack was employed as a model to analyse various technical choices and societal effects. There are many other potential case studies that could and should be considered in a similar approach, which uses the public stack as the basis for critical inquiry into the various layers of technology.

This approach also demonstrates that real and potential gaps in technology exist in each layer of the public stack. There is no single technological component, business model, encryption method, or other individual aspect which could make a piece of technology democratic, fair, and sustainable. To address these problems, we thus cannot try to chase down and tackle every issue we encounter at every layer of every piece of technology that we hope to use. Instead, we have to understand our current gaps and future direction as a holistic problem that begins at the foundation and impacts each layer of design, technology, and citizens.

3. Gap Analysis

- The status quo: The Internet is broken. It is fundamentally undemocratic and fails to protect human rights.
- The ideal future: We want to ultimately have open digital public spaces that allow people to exercise their humanity and citizenship online and, by extension, offline as well. We want these spaces to be based on public values and to ensure the protection of human rights.
- This chapter reviews current progress towards this ideal future and identifies gaps in this progress.

Current Progress

Some of the practical components that we need to develop digital public spaces already exist. Current progress towards this goal includes:

- The identification of some components for designing and developing ethical technology
- Participatory approaches to research and design in technology and governance
- Some experimentation into inclusive data governance models
- Examples of technology that bring some or all of the above assets together and are based on ethical principles and/or made in the public interest and
- Enthusiasm – from citizens, developers, governments at all levels – to make a change and reimagine public space.

Components for ethical technology

There are some existing technological components that can help digital spaces to be private, secure, decentralised, open, and transparent. Existing examples the following:

- **Privacy-by-design** refers to processes that incorporate privacy into the fundamental design of technology. There are various sets of 'principles' for approaching privacy-by-design, notably the *7 Foundational Principles* by Ann Cavoukian[18] and the 'eight privacy design strategies' from Jaap Henk Hoepman's *Privacy Design Strategies: the little blue book*[19].
- **Distributed networks** are networks in which nodes can link directly to one another without being routed through a central hub. In contrast to centralised networks, distributed networks allow for more robustness and relatively more equal access to data (although privileges or restrictions may still be added).
- **Attribute-based credentials (ABCs)** are signed attestations by an 'authority' that vouches for the validity of a set of attributes (of a person) that this authority controls.[20]

[18] https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/

[19] https://blog.xot.nl/2018/05/25/privacy-design-strategies-the-little-blue-book-released/

[20] https://waag.org/en/article/experimenting-attribute-based-credentials

- **Free and Open source Software (FOSS)** is free for all to inspect, use at will, improve and (re)distribute. In essence, it involves the generation of an immaterial common resource through an open collaborative process. Since its inception, the open perspective has migrated well beyond the narrow confines of software. It has been applied to a wide variety of immaterial resources, for example data sets (Open Data BCN, Safecast), encyclopedic knowledge (Wikipedia), hardware designs (Arduino, Local Motors, Open Source Ecology), academic research (Open Access movement), pharmaceutical recipes (Open Source Pharma, Open Source Malaria), and creative works (Creative Commons).

Participatory approaches

Participatory approaches to research and design allow for multiple voices to be brought into a (social, technical, or other) design process. Many recent European projects have utilised participation to deliberately and effectively base technology on shared public values. Multi-stakeholder efforts throughout Europe have helped to familiarise citizens, governments, and civil society organisations with these practices.

- **Co-creation**: Co-creation is a design method that can make challenges of public research into assets. In market research, co-creation has been widely championed as a sound business practice that helps to ensure relevance to customers and an economic reward for corporations. While that is often true, co-creation can also be leveraged to spur collaboration, include a variety of voices, democratise the development process, provide citizens with skills and knowledge, and ultimately help to give citizens agency to implement solutions themselves and alongside public administrations. All of these attributes are beneficial when designing for society, and this makes co-creation a strong method for undertaking **public research** and **public participation**.
- **Citizen science**: Also known as crowd science, crowd-sourced science, civic science, volunteer monitoring or networked science is scientific research conducted, in whole or in part, by amateur (or nonprofessional) scientists. Citizen science is sometimes described as "public participation in scientific research", participatory monitoring and participatory action research.[21] This approach is not limited to the 'natural sciences' but can also be applied to design, problem solving, and social sciences.
- **Public research**: This mode of research prioritises public interest as the guiding principle of innovation, and therefore sees society as its research community. If we want to develop and design for society, society needs to be included in that process. Public research is fundamentally interdisciplinary because it brings together citizens from all walks of life to articulate and address shared matters of concern.
- **Public participation** refers to the involvement of citizens and civil society in public and governmental affairs. Meetups, deliberation & debate, and co-creation sessions often help to facilitate this process.

[21] https://waag.org/en/tags/citizen-science

Data governance models

For digital public spaces, it will be crucial to have a data governance model that is inclusive, respects people's privacy, and allows them to have a say in the process which represents their interests. Current research and experimentation in this area can provide a starting point for considering how data in these digital public spaces might be managed.

Data governance models concern, in a general sense, forms of conditional cooperation around data sources between parties. At the moment there are various ideas in circulation, such as data collaboratives and data trusts. The term 'data commons' is also used in various ways: in most sources it means a general concept of publicly accessible data sources.

With a 'commons' approach to data management, governance is not concentrated with one party but shared among an ecosystem of parties, and a large number of contributors is empowered to use and enrich the platform. Moreover, contrary to a purely 'open' definition, the commons is about finding the right balance between openness and protection of the (knowledge) resource.

Increasingly, there is research into the question of how new approaches to data governance can help to maximise the public benefit of data. This research may be particularly relevant in the development of a data governance model for digital public spaces:

- **NESTA** has created an overview of current research of practices involving data trusts, collaboratives, and coops.[22]
- The **NYU GovLab** has conducted research into emerging data governance models. 'An Introduction to Data Collaboratives' provides an overview of data collaboratives and emphasises their potential to create public value.[23] The GovLab has also published a reading list of 'Selected Readings on Data Governance'.[24] Their article 'Data Governance in the Digital Age'[25] contains a number of readings regarding data governance in the context of Canada, which hold particular relevance for the relationship between existing sovereign governments and new data governance models.
- The **Open Data Institute** published a guide to data trusts which argues for the particular social benefits of data trusts as opposed to other models for data governance.

[22] https://www.nesta.org.uk/blog/new-ecosystem-trust/

[23] https://datacollaboratives.org/introduction.html#section1

[24] http://thegovlab.org/the-govlab-selected-readings-on-data-governance/

[25] http://thegovlab.org/data-governance-in-the-digital-age/

Technology in the public interest

As noted above, there are some existing technological components, open methods, and inclusive data governance models that may be useful when developing an open digital public space. In addition to these individual assets simply being available, there are already a number of inspiring examples of how they have been put together into products, projects, technology, and grassroots initiatives. These examples do not fully meet the qualifications of a digital public space, but nonetheless can provide insight into the possibilities of technology to embody certain public values:

Networks, Communities, and Initiatives

- **Digital Social Innovation** (DSI4EU) (https://digitalsocial.eu/) is an online community to showcase the work of organizations and projects who use digital technologies to tackle social challenges.
- **Gebiedonline** (https://gebiedonline.nl/) is a Dutch 'digital platform that enables local people, groups and organisations to view events taking place in their neighbourhood, share news, exchange and borrow products and services, and meet people. It is a community owned and operated member-based cooperative.'
- **The Bits of Freedom Toolbox** (https://toolbox.bitsoffreedom.nl/overzicht/) (Dutch language) is a set of advice and explanation of commonly-used websites and applications to help people ensure their own safety and privacy when using technology.
- The **Code4All** (https://www.code4all.org/) movement, active in many countries, is an example of an initiative for public software development that contributes to value driven digital public space.
- The **foundation for public code** (https://publiccode.net) enables "public-purpose software and policy that is open and collaborative".

Products and Applications

- **Linux** (https://www.linux.com/) is particularly enabling for the public stack. Many variants of the Linux Operating System are community driven and are very much aligned with public values. It is the world's most widely used free and open source operating system, and is found in 'your phones, your thermostats, in your cars, refrigerators, Roku devices, and televisions. It also runs most of the Internet, all of the world's top 500 supercomputers, and the world's stock exchanges.'
- **Apache** (https://www.apache.org/) software and products are free and open source for the public at large. These projects are 'developed, stewarded, and incubated' by the all-volunteer Apache Software Foundation.
- **Decidim** (https://decidim.org/) is 'a digital platform for citizen participation' and describes itself as offering 'free open-source participatory democracy for cities and organizations'.
- **Your Priorities** (yourpri.org; http://citizens.is) aims to connect governments and citizens through its online platform. It allows people to 'add ideas, view other people's ideas, and take part in a civil deliberation about each idea.'

- **Polis** (https://pol.is/home) 'is a real-time system for gathering, analyzing and understanding what large groups of people think in their own words, enabled by advanced statistics and machine learning. Polis has been used all over the world by governments, academics, independent media and citizens, and is completely open source.' Its use as part of a participatory governance initiative in Taiwan is detailed by the *MIT Technology Review*.[26]
- **IRMA** (https://privacybydesign.foundation/irma-en/) is an app which 'offers a way for privacy-friendly authentication' through the use of attribute-based credentials.
- **Peertube** is an open source video streaming platform that works in a decentralized fashion, allowing everyone to bring up a 'node' and as such can be seen as a building block of the digital public spaces.
- **FairPhone** (https://www.fairphone.com/en/) is a smartphone that aims to be more fair and sustainable than other commercial options by applying modular design, focus on e-waste reduction, and 'fair materials' sourcing.
- **Firefox** (https://www.mozilla.org/en-US/firefox/new/) is 'a free web browser backed by Mozilla, a non-profit dedicated to internet health and privacy.'
- **Signal** (https://signal.org/en/) is an open source messenger app that utilizes end-to-end encryption and refrains from trackers to protect users' privacy. The app does, however, require a connection to a phone number, which has been criticised as a 'major issue' for privacy.[27]

Enthusiasm to reimagine public space

Existing technological capacity, participatory approaches, experimentation into data governance, and examples of ethical technology are all relevant to supply – they point to the possibility to feasibly build digital public spaces.

Demand is equally important. Without it, there would be no need to build digital public spaces. As this report has intended to demonstrate, there is *demand* for these spaces from multiple levels of society that include citizens, governments, tech practitioners, journalists, researchers, and many others which form a yet-to-be-organized coalition of people and groups who are passionate about seeing a positive change in technology.

[26] Horton, Chris. 'The simple but ingenious system Taiwan uses to crowdsource its laws'. *MIT Technology Review*. Article available at https://www.technologyreview.com/2018/08/21/240284/the-simple-but-ingenious-system-taiwan-uses-to-crowdsource-its-laws/

[27] https://theintercept.com/2017/09/28/signal-tutorial-second-phone-number/

Current Gaps

Some of the individual components that we would hope to see in a digital public space already exist, are being built, or are studied in some form, but they have not been brought together in a way that is reflective of true public spaces. **To achieve this, we need**:

- **A shared vision and mission**

A journey towards the development of digital public spaces requires a shared vision and mission so that the various groups and people who contribute to this effort can do so in a unified way. As is the case with many aspects of this effort, a shared vision and mission cannot come from a single source but rather need to be iteratively co-created as part of a community effort. Based on our research we propose a vision and mission in the next chapter that we believe can form the basis for this exploration.

- **A shared foundation, 'set of values' and/or 'digital social contract' that can underpin the development of technology**

A shared set of public values needs to form the foundation for digital public spaces. This foundation needs to be developed as part of an open, fair, and democratic process. The 'public stack' model can serve as guidance to understanding what various aspects we need to address in order to define a solid foundation for our digital public spaces.

- **A clear and concerted effort to democratically bring these elements together into a feasible and inclusive movement**

While the enthusiasm for such a movement currently exists, it is still fractured among distinct and unconnected communities and has not yet been brought together or mobilised. We currently lack a cohesive movement which attracts the wide range of people who are passionate about ethical technology and have the means to make digital public spaces a shared reality. A movement of this sort needs participation from multiple groups in society, including citizens, governments, and developers.

- **A shared digital infrastructure that begins the process of developing online public spaces in a way that can be adopted and adapted locally while also being interoperable internationally.**

We currently lack a shared scaffolding that like-minded people and organisations can contribute to when developing technology based on public values. Rather than having an ecosystem technology where individual efforts can influence and build upon one another, the status quo often leaves such efforts in isolation – sustainability, uptake, and user experience all suffer as a result of this fragmentation.

For digital public spaces to become a reality, there needs to be a shared technical framework within which they can be developed, experimented with, and grown. Within this shared framework, guided by its shared rules and guarantees, people should be free to design their own technology.

- **An active digital sphere where these efforts can come together and be presented.**

Citizens online today may not know where to look to find technology that aligns with their values. Even when they have the feeling that the technology they currently use, the vast array of options, conditions, and varying sets of protections makes the question of 'choice' far too difficult – even for the 'experts'! *Citizens should be able to live, work, and interact in a digital sphere where they can be assured that certain values are upheld consistently and assured through sound technology.*

4. Next phase

- Chapter 1 provided an overview of public values that a digital public space could draw from, and argued for an outcome in which these public values form the foundation for new technological development.
- Chapter 2 presented an exploration of two use cases (video conferencing and identity in social media) to get a better sense of what digital public spaces could be in terms of technology, design, and public values.
- Chapter 3 provided an overview of existing components, methods and gaps for building a digital public space
- This chapter introduces our vision and mission and explains the first steps towards the realisation of this mission.

During the phase reported here we mapped the public values for building digital, public spaces in Europe. We conclude that a digital public space needs to be open, democratic and sustainable. Furthermore, we analysed potential partial solutions that help us move towards digital public spaces, created a visual narrative and performed a gap analysis.

Based on our research and conversations, we are confident there is sufficient overlap, and connection points between the various initiatives to develop a coherent overarching vision and mission for digital public spaces, which we propose to be as follows:

Our **vision** is the realisation of open, democratic and sustainable digital public spaces.
Our **mission** is to create open, democratic and sustainable digital public spaces by 2025, both locally and in Europe.

In the next phase we build upon our research and the results in order to get a step closer towards the realisation of this mission. We specify three tracks to lay the groundwork for this:

- Track 1: the development and mobilisation of an inclusive movement
- Track 2: the creation of some key building blocks of a shared digital infrastructure
- Track 3: the realisation of a digital public space on a local level (in Amsterdam)

In this chapter the tracks will be further explained and followed by an overview of the corresponding activities.

1. The development and mobilisation of an inclusive movement

During the preparatory phase we spoke with a broad range of people and organisations committed to the ideals of digital public spaces. As defined in the gap analysis, we see an urgent need to bring these organisations and initiatives together under a shared mission. Part of our mission will therefore be the development and mobilisation of a movement that endorses the mission of open, democratic and sustainable public spaces. This movement needs to appeal to a wide range of people, organisations, and communities, so that the movement itself is a fair representation of the society for whom the digital public spaces are intended. Also, we will seek connection and alignment with other relevant organisations and coalitions with related or similar missions not yet mentioned in this report; for example the recently announced European Public Sphere Alliance[28]. Finally, any civil society organisation or representative from civil society that strives for the creation of a digital public domain on the basis of the identified values is welcome.

The purport of this movement is that every affiliated initiative endorses the vision and the mission and defines their own contribution to the movement. These contributions can differ in many aspects but align and relate to the vision and mission. For instance, some organisations' missions are committed to the development of ethical technology where others are focused on safeguarding human rights in the public domain.

At the same time, we aim with this movement to enhance the visibility and 'findability' for other initiatives and organisations. Initiatives can, as part of the movement, create sub-alliances in order to pursue a more specific agenda, for example on specific topic areas such as identity management, specific public domains such as healthcare or education, or operate within a specific geographical context. An example of the latter is the development of an alliance to work towards a digital public domain in Amsterdam (see track 3). This type of alliances leads to new partnership and new formations and could therefore attract new initiatives to be part of the movement.

[28] https://en.acatech.de/publication/european-public-sphere/

2. The creation of some key building blocks of a shared digital infrastructure

In this track we will create a first blueprint of a shared digital infrastructure. A new shared digital infrastructure must address at least three topics, the so called 'building blocks' for a new digital public space. We explain shortly the need for the conceptualisation and creation of these three building blocks here. These build on our research on the use cases and can be seen as prerequisites for developing applications and end-user services in the public digital spaces.

The technology supporting a digital public space needs to be public itself, in some form, mainly from the perspective of **governance**. Not only the artefacts in the public space need to be 'governed', but also the technology and the sustainability models that enable the public space itself. Governance of the digital public space in general will necessarily be extremely complex given the multitude of interests that need to be balanced in various domains and with respect to countless resources. Governance is a process, driven by a model. And in the case of a digital public space unavoidably facilitated by technology from the start. In order to operationalise this idea somewhat, we need to be able to speak about **who** and about **what**. When we want to match interests to resources and capabilities we need to formalise the who and the what, leading to two further building blocks of the digital public space: **identity** and **data (resource) management**.

Taking a step towards a sustainable practice of design and development we come to these three fundamental building blocks that we each see as a collection of services.

I. Governance services

Governance services will facilitate bringing together the actors and the resources in the digital public space, both in an active and in a passive capacity. The actors, be they individual people or communities, public institutions or other entities are both the subject of the governance process as well as a driving force in that process itself. Without relying on technology in a naive or overly optimistic way, we will need to research ways in which technology may be able to assist in what would otherwise be unmanageable, at least when considering the precision that we think is needed (think medical records, for instance). A simple-minded rule-based system is unlikely to ever be finished with the required completeness and precision. Semantics-based meta rules, segmentation and alignment of interests, delegation and representation, these are subjects where technology might assist. What is also needed is a re-evaluation of existing liquid democracy tools as well as a comprehensive domain ontology.

II. Identity management services

What identity services do we need for resource management and governance? Identity is a bit of a misnomer as we will hardly ever need to be concerned with identity. What we will be looking at is a very granular, attribute based authentication and digital signing, based on verifiable credentials. The various attributes will be issued by specific authorities (not necessarily, but possibly including, national or local government), which may, analogous to the SSI (self-sovereign-identity) concept, form, possibly domain specific, hierarchies of trust. Identity, here, will be more of an emergent property based on domain, actions, positions taken, and resources managed. Given a robust authentication and signing capability will enable authoritative answers to questions of ownership and provenance, will facilitate privacy and security by design, and will also enable fine-grained governance and data management services.

III. Data and resource management services

Many initiatives have considered data and resource services, of course. Starting in earnest with the open data movement the narrative has evolved into a much broader vision of data with a more nuanced open versus closed consideration. After all, when discussing data in the context of a DPS value is found in all data that is not strictly private and is sharable under specific conditions; not only open data. Data, in combination with a fine-grained ownership and usage model enabled by the identity services discussed earlier, is a key enabler of the DPS. Data is not the only resource that needs management in the DPS, however. We think of community platforms like health or neighbourhood platforms, digital representation of NGOs or non-commercial social media or news platforms and much more.

In order to be able to match identities (entities) to data, resources and capabilities we need to be able to specify these in a robust fashion. The second (identity) is addressed earlier, the others are in need of an organisational principle which allows us to specify, find and talk about them. We will be looking at Solid and dat:// , for instance, but other (semantic) technologies may be relevant. Federation and distributed file systems are relevant keywords as well.

Substantial effort has been spent by many on all of these already, in various contexts. What we propose is to consider these under a common narrative, and, working through selected use-cases, fill in the needed gaps and make a start towards the development **of a community of practice** that would continue design and development and refine existing efforts in order to be able to take concrete steps towards a open, democratic and sustainable digital public space.

3. The realisation of a local digital public space in Amsterdam

While mobilising a movement and creating a digital public infrastructure, in track three we will develop and experiment with the provisional results of the other tracks at a local level in Amsterdam.

In Amsterdam we will dive into the Amsterdam context and the idea of Amsterdam citizenship. Waag, as a Future Lab in progress[29], has a close relationship with the municipality and local (cultural) organisations. It has had a pioneering role in creating a digital public space in the early nineties by creating the 'Digitale Stad'[30] and still has a leading role regarding safeguarding values of openness and democratisation while becoming a 'smarter' city. Our ambition is to shake the dust off this still groundbreaking idea of creating a digital city and realise a new digital public space, fit for the 21st century.

Over the last few years, the first crucial steps have been made by local initiatives such as tada.city[31], cities for digital rights[32], public roam[33], data commons[34] and other creative makerspaces.

---

[29] https://waag.org/nl/article/raad-voor-cultuur-adviseert-waag-als-future-lab-design-technologie

[30] https://waag.org/nl/article/marleen-stikker-over-25-jaar-digitale-stad-we-moeten-het-internet-heroveren

[31] https://tada.city/

[32] https://citiesfordigitalrights.org/

[33] https://publicroam.nl/

[34] http://datacommons.nl/

On a different level, the municipality of Amsterdam has embraced Kate Rayworth's doughnut model that strives for Amsterdam being a regenerative and inclusive city for all citizens while respecting the planet. The recent history of the city, the local initiatives and the announcement made by the municipality form a fruitful foundation for the creation of a new digital public space in Amsterdam. Currently, Waag is already working on the development of this local coalition of key players to jointly develop a roadmap for the next five years to build the Amsterdam digital public space.

The creation of this new 'digital city' requires the involvement of a broad range of societal stakeholders. We will invite parties varying from neighbourhood initiatives to key public domains and public actors, such as the local library and schools, representatives of city districts, local organisations and so forth. The required activities to fulfil this mission are described below. We will seek collaboration and exchange with other similar initiatives in other European cities and places, so we can learn from each other and jointly spread these initiatives across the European continent.

Activities

The creation of digital public spaces that are open, democratic and sustainable requires activities in three different tracks. Every track has different activities that we break down in various phases. The table on the next page suggests example activities across the various phases that we propose in the follow-up project. There will be some level of iteration based on the findings from the other tracks.

We plan to discuss and work out these phases during the coming months by validating our identified vision and mission with the consulted stakeholders. In order to make our movement inclusive and successful we need to take into account the strategies and agendas of similar initiatives. Our activities will therefore be researched and specified in the coming months.

	1 Inclusive movement	2 Digital infrastructure	3 DPS in Amsterdam
Phase 1: Rallying around a shared mission	(Re-)approaching organisations and confirming their endorsement of the shared mission and their role in development of the digital public spaces	Defining the social contract for the digital infrastructure based on the agrees values applying the public stack model	Gathering relevant public actors and domains for creating local digital public spaces in Amsterdam
Phase 2: Building the foundation for the digital public spaces	Gathering committed organisations and further defining how their contributions can be combined and complemented	Concretely defining and developing the identified building blocks of a digital infrastructure based on the Public Stack into a *European blueprint* for Digital Public Spaces	Defining the needs and roles of the various partners of the Amsterdam local digital public space based on the European blueprint
Phase 3: Developing digital public spaces	Spreading the movement to parts of Europe and beyond that are not yet represented, building new alliances and relationships.	Further developing a European blueprint with delegation of movement. The blueprint leaves attributes open reserved for local adjustment Developing, assessing and iterating use cases (on the three building blocks) with delegation of movement.	Building applications and platforms that fulfil the use cases relevant to the Amsterdam stakeholders together with these local organisations
Phase 4: Further maturing and spreading the digital public spaces	Sharing our results in conferences and further building out the movement based on these key outcomes	Developing, assessing and iterating use cases (on the three building blocks)	Organising a campaign in Amsterdam on the local digital public space and gaining commitment of various public institutions to make use of the developed building blocks

Appendix 1. Explanation of the investigation

Waag has initiated this process through the OEPS research project: identifying the key values driving our shared current and imagined public space (chapter 1); grounding the technical and social discussion in real-life use cases (chapter 2); considering the limitations and affordances of existing technologies' potential contributions to a public stack (chapter 3); and presenting options for further research and development (chapter 4). The outcomes of this research are made available in this report and at www.waag.org.

Our research into values, use cases, and communities was guided by a series of interviews, group discussions, and conversations with people from across Europe who work in a number of fields related to society, digitalisation, and public space. The goal of these interviews was to map the European public values that people from diverse areas of expertise consider to be most important with regard to our shared online spaces. This included media professionals from across Europe; academic researchers of data commons, data rights, digital activism, and digital spaces; and activists and practitioners in the field of ethical technology. These interviews were supplemented by previous co-creative research conducted by Waag to identify key values for technology held by **citizens** and **public administrators**, specifically through the DECODE project (https://decodeproject.eu/) and Digital Identity Lab (https://policylab.waag.org/).

In addition to these conversations, desk research was also conducted into multiple areas of focus:

- Case studies
- Video conferencing platforms
- Digital identity
- Open source technology
- Ethical technology
- Organisations, projects, and social movements which are both directly and indirectly aligned in advocating for an Online European Public Space

Hands-on experimental research was conducted or through:

- Experimentation with various video conferencing platforms
    - Testing a number of 'alternatives' with various ratios of functional/ethical
    - Installed and hosted a (open source) Jitsi platform for use by the general public
- Ongoing collaboration (stemming from previous projects) with the Amsterdam municipality to develop digital resources for privacy-friendly identification systems.

Appendix 2. Values from independent initiatives

- **Tada** (https://tada.city/en/home-en/): 'Professionals from the Amsterdam region...wrote a manifesto entitled 'Tada – data disclosed'. Government authorities, companies and other organizations from different regions are invited to use and sign the document, showcasing their ambitions to shape a responsible digital city.' The Tada Manifesto includes 6 principles:
    - Inclusive
    - Control
    - Tailored to the people
    - Legitimate and monitored
    - Open and transparent
    - From everyone – for everyone
- **Cities for Digital Rights** (https://citiesfordigitalrights.org/): The 'Cities Coalition for Digital Rights aims to protect and uphold human rights on the internet at the local and global level.' The coalition lists 5 principles:
    - Universal and equal access to the internet, and digital literacy
    - Privacy, data protection and security
    - Transparency, accountability, and non-discrimination of data, content and algorithms
    - Participatory Democracy, diversity and inclusion
    - Open and ethical digital service standards
- **PublicSpaces** (https://publicspaces.net): PublicSpaces has the mission to '[reclaim] the internet as a force for the common good and [advocate] a new internet that strengthens the public domain.' Their manifesto specifies 5 values & principles:
    - Open
    - Transparent
    - Accountable
    - Sovereign
    - User-centric
- **Mozilla Manifesto** (https://www.mozilla.org/en-GB/about/manifesto/): Mozilla, perhaps best known for its Firefox web browser, has the stated mission to 'keep the internet open and accessible to all.' The Mozilla Manifesto contains 4 core tenets:
    - We are committed to an internet that includes all the peoples of the earth — where a person's demographic characteristics do not determine their online access, opportunities, or quality of experience.
    - We are committed to an internet that promotes civil discourse, human dignity, and individual expression.
    - We are committed to an internet that elevates critical thinking, reasoned argument, shared knowledge, and verifiable facts.
    - We are committed to an internet that catalyses collaboration among diverse communities working together for the common good.

The Mozilla Manifesto also includes 10 principles:

- The internet is an integral part of modern life—a key component in education, communication, collaboration, business, entertainment and society as a whole.
- The internet is a global public resource that must remain open and accessible.
- The internet must enrich the lives of individual human beings.
- Individuals' security and privacy on the internet are fundamental and must not be treated as optional.
- Individuals must have the ability to shape the internet and their own experiences on it.
- The effectiveness of the internet as a public resource depends upon interoperability (protocols, data formats, content), innovation and decentralised participation worldwide.
- Free and open source software promotes the development of the internet as a public resource.
- Transparent community-based processes promote participation, accountability and trust.
- Commercial involvement in the development of the internet brings many benefits; a balance between commercial profit and public benefit is critical.
- Magnifying the public benefit aspects of the internet is an important goal, worthy of time, attention and commitment.

- **Shared Digital Europe** (https://shared-digital.eu/vision/): 'This document summarises the efforts undertaken by Kennisland, Centrum Cyfrowe and Commons Network to develop a new vision for digital policymaking in Europe. To this end, [the authors] have created a new policy frame, in an effort to find solutions for a number of problems that plague the Internet.' Relevant to OEPS, the vision statement says, "Europe needs to establish its own digital space that embodies our values: strong public institutions, democratic governance, sovereignty of communities and people, diversity of European cultures, and equality and justice. A space that is common to all of us, but at the same time diverse and decentralised." The document presents the following core values and principles:
  Core values:
  - strong public institutions to protect the digital space and people's digital lives;
  - democratic governance and control of these public institutions to ensure individual and community sovereignty;
  - cultural diversity and space for creativity and initiative to maintain and strengthen Europe's innovative edge;
  - human rights and social justice ensuring that all Europeans have the actual opportunity to enjoy the digital space equally.

  Four principles:
  - A shared digital Europe enables self-determination
  - A shared digital Europe cultivates the commons
  - A shared digital Europe decentralises infrastructure
  - A shared digital Europe empowers public institutions

- **Open Data Institute (ODI)** (https://theodi.org/about-the-odi/our-vision-and-manifesto/): ODI 'envisions a future where people, organisations and communities use data to make better decisions, more quickly...To bring about this future, we must make data as open as possible while protecting people's privacy, commercial confidentiality and national security.' Their manifesto includes six areas of focus:
    - Infrastructure: Sectors and societies must invest in and protect the data infrastructure they rely on. Open data is the foundation of this emerging vital infrastructure.
    - Capability: Everyone must have the opportunity to understand how data can be and is being used. We need data literacy for all, data science skills, and experience using data to help solve problems.
    - Innovation: Data must inspire and fuel innovation. It can enable businesses, startups, governments, individuals and communities to create products and services, fuelling economic growth and productivity.
    - Equity: Everyone must benefit fairly from data. Access to data and information promotes fair competition and informed markets, and empowers people as consumers, creators and citizens.
    - Ethics: People and organisations must use data ethically. The choices made about what data is collected and how it is used should not be unjust, discriminatory or deceptive.
    - Engagement: Everyone must be able to take part in making data work for us all. Organisations and communities should collaborate on how data is used and accessed to help solve their problems.
- **Amnesty International's 'Artificial Intelligence and Human Rights'** (https://www.amnesty.nl/wat-we-doen/tech-en-mensenrechten): The Dutch chapter of Amnesty notes that: 'Because many systems are not transparent or have been developed with the wrong vision, they can make decisions that have major consequences for our private life. Violating our privacy is a major risk.' To this end, Amnesty has formulated four points:
    - A binding human rights test – Before algorithmic decision-making and AI are procured, designed, developed and used, a binding human rights test must be conducted. Such a test must also be carried out regularly during further use.
    - An algorithm watchdog – An algorithm supervisor should oversee how algorithmic decision-making and AI respect, protect and promote all human rights, including socio-economic human rights. The supervisor must have access to the data and algorithms to investigate the systems and outcomes.
    - Transparency – There must be transparency about the data, the algorithms and the effect of the algorithmic decision-making on the consequences for an individual.
    - No self-learning algorithm in the performance of government tasks that affect an individual – Government action must be verifiable and predictable. Automated decision-making should be verifiable when it has legal consequences, when it affects individuals significantly or when it has a major impact on people or society. The use of self-learning algorithms means that government action cannot be properly controlled. As a result, these self-learning algorithms do not suit the performance of this type of government task.

Appendix 3. Case Studies

Case study: Identity management

Introduction

Considering Digital Identity in the context of the public stack, we see the subject represented in all layers, and firmly rooted in the **foundation**. Identity and its related concepts of ownership, authenticity, anonymity and privacy are a very integral part of the foundation on which systems and processes are designed. Some of the most important core values we consider in the digital domain, related for instance to the **UDHR**[35], revolve around concepts related to, or requiring a notion of, identity. The very actual questions around self-sovereign identity and data vaults and current efforts to formalise online IDs from an administrative perspective are testament to the very active **governance** discussions around digital identity.

We **design** for entities that we need to be able to talk about and address and that need to be able to interact amongst themselves. We design for privacy or for access for somebody who has to be defined and addressable in some way. And in our design we consider how much identity we require for the systems under consideration, where a scope from fully anonymous to fully identified is available for every aspect of our design.

In the implementation of **technology** and services we again see the need for a flexible and nuanced notion of identity, from the **hardware** layer – in cryptographic systems you are represented by keys or functions, implemented in a usb dongle or a TPM[36], for instance, or more fancifully in PUF's[37] – all the way to the services and application layer where identity is not only a very profitable business case for social media platforms, buy also a means of artistic expression for some. Here we have arrived at the top of the stack where we, as **citizens**, currently have only the thinnest thread of control. Designing (for) the public stack aims to correct that and make truly public digital spaces possible.

Identity and authenticity

The process starts in the foundation; this is where we decide what we see as the core values underlying the concept of the public space, how we govern it, sustain it and for whom. While much can and should be said about these topics, this section will focus on one specific value and try to follow its implications going up the stack: **authenticity**.

We engage in the public space; we consume and we produce. We express, communicate, learn, teach, influence, or simply let ourselves be entertained. Whether we consume or produce, in essence we engage in a relation. This could be one-on-one or one-to-many, it could be a conscious relation or an implicit one, and it could be real-time or take place across years or decades.

---

35 https://en.wikipedia.org/wiki/Universal_Declaration_of_Human_Rights

36 https://en.wikipedia.org/wiki/Trusted_Platform_Module

37 https://www.embedded-computing.com/guest-blogs/demystifying-the-physically-unclonable-function-puf

There are occasions where we do not care about the other parties in the relationship – we simply interact. At the same time we may not care for the other(s) to know us, we might want to be anonymous, or maybe our whole purpose is exactly not to be anonymous. Or maybe we have a carefully crafted alternate identity for a specific context.
It is vital to realise that for all parties involved this is a *continuous scale*; from fully anonymous to fully identified, and that all positions on this scale fulfil proper and important needs, sometimes needs that have life or death consequences (think of critical journalists in some countries).

Authentication and protocols

If we take a leap of faith and suggest that online public spaces can be defined through a set of *values, governance rules, design principles and protocols* (going up the **public stack**), we see that in the **protocol** sphere we can (and should) facilitate this continuum of identification. Through *verifiable credentials* we can disclose *attributes* of ourselves which can be tuned to the circumstance with arbitrarily fine granularity. See IRMA[38] for a mature implementation of this approach to authentication.

Currently, these approaches are mostly used or imagined in the context of *authentication*; i.e. in cases where access to a resource or platform needs to be limited to a specific set of users. A social security number for access to my tax statement form, a verifiable statement of residence for a municipal questionnaire. This approach works well in conjunction with the GDPR data-minimisation requirements, and is an important step in assuring that our digital public space does not become a free-for-all personal data collection opportunity.

An equally important opportunity previously mentioned protocols offer is their application to *authenticity*, both of media and of participants. We live in an era of spam, bots, conspiracy theories, deep fakes and fake news. The social media platforms delete billions of fake accounts as a matter of fact, but miss billions more. Spam and phishing mails cost 100's of millions each year. Cleary, a naive concept of a public space anonymously open to all will face some serious challenges.

Authenticity and reputation

Consider the authenticity of participants in practice. As an example of a hypothetical platform in an online public space, imagine a health platform that is concerned with some particular ailment. The forum is open to everyone, but participants are potentially labelled as medical professionals, sufferers of the particular affliction or a family member of such. These labels are *verifiable*, meaning that there is an "authority" that underwrites that particular claim. For doctors this is the health board, for sufferers it may be the hospital or medical specialist, and for family members it would be the patient. This is all arranged at the protocol level and highly automated. The result is that discussions and experiences can be relatively anonymous, but participants can see at a glance (with a visual indication for instance) how to judge and interpret contributions. We do not need real names to participate authentically. Without such a label participants can still join the discussions, but if one of them starts to praise the incredible effects of a particular medicine but is not labeled as a patient or specialist, people will be able to better judge the validity of these claims and maybe suspect commercial motives.

[38] https://irma.app

The implications of the use of these technologies need to be considered carefully, however. Naïve (technical, but, more importantly, social) implementations could lead to very undesirable effects. As an example, we can explore a non-platform-specific quality in dire need of authenticity: **reputation**.

We might be familiar with the troublesome ratings mechanisms of hotels, restaurants or online retail platforms' product reviews. These are highly manipulable and can cause businesses severe headaches or worse, apart from potentially misleading customers or clients.

But, more relevant to the current subject, people also carry a reputation as part of their identity. Operationalised reputation is very important, for instance, for a worker in the 'gig' economy where it has a direct impact on the availability of work and income (Temper, Uber), but also in a more general sense, as a car-sharing user, an airbnb guest or host, or as an expert on a technical forum such as stackoverflow.com.

There is no question that it would be very useful when reputation (both of businesses and people) could be trusted to be authentic, and personal reputation could be made portable across platforms. A trustworthy and careful airbnb guest may be relied upon to also take good care of the car you share with them. News items written by a peer-rated anonymous journalist might be taken more seriously than any old posting online.

Even though these ideas are about people substantiating claims they make about themselves (as opposed to the Chinese social credit system where claims about you are made by others - the state) the social effects could be similarly undesirable when generalised high reputation scores become a requirement for social participation. Careful research, discussion and design need to lead to social and technical (protocol-level) implementations and schemas that will make an approach to *reputation* robust against these sorts of effects and abuse.

Verifiability

Lastly, public spaces are not only populated by people, businesses and systems, but also by data and media. Somewhat related to the previous topic of reputation, media is data produced or collected by someone, and with a purpose. Media is shared, adapted, changed or manipulated (or not), by someone else and again with a purpose.

Until the advent of 'social' media and the internet in general, the medium carried (and still does) the reputation, and provides a certain context. An item in a tabloid would be read in a different frame of mind than an article in a 'quality' newspaper or an item on BBC news. As the source of messages (and data) becomes more diffuse, the context in which they are to be consumed is lost as well. This confusion has traditionally been exploited, of course, by the advertising industry, where a message is presented with a particular frame of reference (i.e. scientific, or 'young happy people') instead of the objective one of the business that needs to sell a product.

Digitally signing a message has been possible for a long time. This would let anybody know from whom the message originates. This is less relevant in the context of commercials, as we know the message comes from the manufacturer of the tooth-paste, but more relevant in the current era of politically motivated (dis)information and deep fakes. We lack an infrastructure to do so, and to do so with the needed granularity and the needed safe-guards for privacy.

We do not need a full disclosure identity for all media at all times; when we can sign our messages with certain attributes this can already go a long way towards interpreting them in the right frame of reference. When we know (verifiably) that the item comes from a peer-accredited critical journalist-blogger, we do not need to know the name, especially not when she is working in a dangerous environment. The verifiable tag 'Dutch national' helps fight fake accounts on social media, as does the tag 'medical professional' in qualifying contributions on an online forum. The approach is the same as the one needed for the earlier mentioned verifiable credentials, infrastructure and user-level design challenges are huge, but first steps have been taken.

We cannot expect or require all media to be tagged or signed, but we do know that untagged messages are just that, and can then read or watch them as such.

Although we cannot be too optimistic in the knowledge of state-level meddling, we can hope that verifiable 'tags' on media are a start towards more confidence as regards the provenance of media and data and the frame in which to interpret them.

Case study: Video conferencing

Introduction

This section discusses video conferencing tools using the layers defined in the public stack model. Firstly, we will focus on the main technological features of video conferencing tools. We then offer a perspective from the users' point of view (the citizens perspective), by showing how the different technological choices relate to design decisions and trade-offs. In order to prioritise the different design options it can be useful to look at the foundational layer of the public stack.

Questions such as for whom the tool should be suited, who defines a successful tool, whether user privacy is guaranteed, and what the business model of the tool provider is can be used to identify which characteristics are important and which tools should be chosen.

The technology stack

A generic video conferencing solution can be implemented by several technical components that form a rather complex system. In order to simplify the discussion about the properties of such systems, we can group the functionality in two main components, whose interaction provide the video conferencing service to users:

- The **client**: This is the application with which the user interacts and it is a required component for video conferencing. An example of this is Whatsapp installed on a user's mobile phone.
- The **server**: This can be thought of as an application that runs on a machine different from where the client runs. The client application may interact with the server to use particular services for video conferencing (more on this later). A server is not always required, and it is normally not explicitly visible for a user, since the interaction with it is taken care of by the client application. It is important to stress the role of a server since users tend sometimes to think that they are directly connected to another user when video conferencing, but their communications often go through a server.

There are mostly two different classes of client applications clearly distinguishable for users: video conferencing that runs in a web browser, and video conferencing that requires one to install an application.

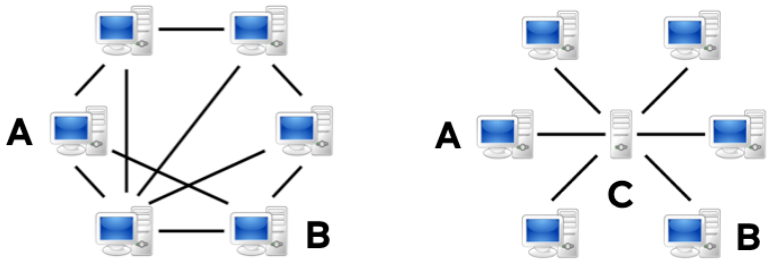
One clear difference is that the former has a lower threshold to use, as the extra step of installing the software is not required. This makes the in-browser option preferable, but it also means that such tools have less "freedom" to operate, since they are constrained by the functionality offered by existing browsers. Usually this functionality is the product of a standardisation process, which has the advantage that this functionality is uniform across different browsers, but the disadvantage that adoption of new features can be slow.

On the contrary, an application can use all the functionality that an operating system (such as MacOS, Windows, Linux) can offer. This fact can be exploited for "good" (e.g. to offer stronger encryption) or for "bad" (e.g. perform operations that are more invasive for the privacy of the user).

The Infrastructure layer

The infrastructure layer is particularly interesting for this use case as it reveals what plays behind the scenes. We consider this layer to encompass the network and the servers that make video conferencing possible.

User devices such as mobile phones need to establish a connection in order to communicate with each other. These connections are carried over a network, such as the mobile telephone network for mobile calls, or the internet for calls such as for Skype calls. If we abstract from the physical devices implementing these networks and apply some degree of simplification, there are two main types of network configurations, peer-to-peer configuration and client-server configuration.



In the peer-to-peer configuration, client applications are connected directly to each other. This means that the data (i.e. the audio and the video) is exchanged directly between the participant to the video call, e.g. A can talk directly to B.

In the client-server configuration, the data goes through a server. This means that the data transits through a third party before reaching its final destination. In this case A cannot talk directly to B without passing through server C.

Peer-to-peer offers theoretically more privacy as there is no third party involved in the communication, but there are more tasks that each client has to perform as it can not rely on the services offered by a server. We explain further what the role of a server can be in the following section.

Context layers

We now take a look at video conferencing as a service that involves different aspects.

There are two main phases in video conferencing:

1. Discovering who you can talk to and establish a connection (we call it **signalling**)
2. **Communicate**, i.e. exchange video and audio data in real-time.

The first phase can be thought of as "looking somebody up in an address book and calling them", while the second phase starts after the called party replies and the conversation can start. We explain how these two phases differ in the peer-to-peer and client-server network configurations.

Peer-to-peer signalling

In a peer-to-peer configuration each client needs to keep track of who the other clients are on the network, and continuously listen to incoming calls. There is no central server where clients can report their presence to, and ask who else is online (like what happens with Skype for example). There is also no central location where users can connect to at the time of an appointment they have previously made.

This implies that each client continuously sends and receives data in order to be aware of who is online. Clients need to perform more work and this scenario is generally more difficult for resource-constrained devices, such as mobile phones.

Peer-to-peer communication

When a connection is established, clients can communicate with each other in the communication phase. In a conversation each client transmits directly to each other client node. Since there is no server involved, there is also no resource bottleneck due to a server's processing power or network bandwidth.

The limitations are just each client's bandwidth and processing power. Of the two, the main limitation is the bandwidth, since in a conversation with N parties each client receives N-1 audio/video streams from N-1 parties and sends out N-1 audio/video streams to as many parties. In the picture above with 6 parties, A needs to hear the voice and see the video of the other 5 parties, and send its own audio and video to these 5 parties.

Client-server configuration

It might seem that, although with some difficulties for the signalling part, a complete peer-to-peer video conferencing is possible with no server needed. In practice peer-to-peer communication is also difficult to achieve because of the security constraints in network communications. This is because for security reasons often clients are connected to the internet using a mechanism (NAT[39]) that hides their real address (their IP). It is therefore impossible to directly connect to them. This limitation requires the use of services provided by external servers, which for example allow clients to connect to them and exchange data[40].

So although peer-to-peer is theoretically possible, it is difficult to achieve it for both the signalling and communication phases. A server (likely run by a third party) is often needed. Usually a solution can therefore be peer-to-peer only to a certain extent (see for example Jami), and rely for the rest on centralised means. To give an idea, also the privacy-preserving Signal app requires servers for the signalling phase and sometimes also for the communication phase.

---

[39] a NAT (Network Address Translation) server masks clients' IPs and presents to the external world its own IP. In most NAT versions, such clients cannot be reached by connections initiated outside the NAT perimeter, but they can initiate a connection. If both clients are behind a NAT, there is no way that they can talk directly to each other.

[40] STUN servers provide a mechanism to discover a client's public address, and might work with particular types of NATs. TURN servers provide a mechanism to route all traffic through them, and work when STUN is ineffective.

Security

Here we interpret security as security of the communication, ie. its privacy. More general security considerations will be given in the citizen perspective section.

Given that in most cases video conferencing data needs to go through a server, this server should know as little as possible to preserve the privacy of the users. There are two types of threats:

1. A third party knows who talks to whom since it can observe the signaling phase
2. A third party knows the content of the communication since it can observe the communication phase.

The first one can be handled with systems like Tor[41], but it is generally considered to be less sensitive. The second one is usually tackled by encrypting the data. There are two types of methods:

1. Transport-level encryption: the data is encrypted between the client and the server
2. End to End encryption: the data is encrypted from client to client

The first method can protect against snooping of the network traffic, but the server can still see the data. This kind of protection is the same as when visiting a website with a URL starting with HTTPS. The communication is protected but the server can of course see the content.

With the second method, only the clients can see the content of the communication, and it is therefore preferable. Again, this comes with more work for clients, since clients need to manage the encryption with their own resources, with no help from the server as this would imply that the server can see the content. For example, in the past there have been cases of "fake" end-to-end encryption with Zoom: the server was choosing the encryption keys and distributing them to every client.

End-to-end encryption prevents the server from providing several services that would require access to the content, such as recording the meeting, or allowing people to phone in. Intelligent functions such as detecting who is talking in order to optimise the bandwidth are also not possible.

At the moment there are few offerings for end-to-end encryption. Among the commercial ones Whatsapp and WebEx support it, and in the open source Jami[42] and Signal. Of the most known open source solutions, Jitsi[43], SylkServer[44] and BigBlueButton[45], none supports (yet) end-to-end encryption. When using these services you therefore need to trust that whoever runs the server (in case it is a third party) will not spy on you. In some cases you might trust the server more than the party you are talking to: Signal for example routes your communications to a party who is not in your address book via their servers, in order to not disclose your IP to the other party. On the other hand, trusting organisations that are well-intentioned does not mean that the communication is secure, since that depends on how many resources the organisation running the service can dedicate to secure it against attacks from hackers.

---

[41] https://www.torproject.org/

[42] https://jami.net/

[43] https://jitsi.org/

[44] https://sylkserver.com/

[45] https://bigbluebutton.org/

Protocol and standards

Most of the solutions that are browser-based use a standard called WebRTC, which has allowed browsers to become platforms for real-time multimedia communication. The origins of WebRTC are traced to when Google acquired a videoconferencing software company and subsequently open-sourced its technology, with the intention to propose it as a standard to bodies such as the W3C and IETF. As of today, WebRTC is a W3C Candidate Recommendation. WebRTC has therefore played a role of an enabler for further applications to be developed for every platform where a browser could run.

On the other hand, WebRTC does not support end-to-end encryption yet, although there are plans to develop it. So no WebRTC-based video conferencing tool can be end-to-end encrypted. As already noticed above, this is a downside of using standards, which can be slow to adopt innovations.

The citizen perspective

Looking from a final citizen perspective, there are two groups of characteristics of video conferencing tools that have consequences for users.

The first group is directly noticeable for users as it contributes to the user experience:

1. The tool's ease of use
2. The richness of features of the tool, such as recording the session, or allowing dial-ins via phone.
3. Accessibility, such as from resource-limited devices, or for people with disabilities.

The second group still has consequences, but these are less noticeable

4. Privacy
5. Security

The first two characteristics are the most used ones when choosing a solution with respect to another one. Nevertheless, the third one should also be considered if the goal is to be as inclusive as possible. What is easy to use for a user with normal capabilities can be hard for a visually impaired one. For example, Jitsi was found difficult to use for blind people, as the tool uses many visual clues which are not readable by a screen reader.

Further, there can be a certain tension between the first group and the second one. Ease of use, features and accessibility for resource-limited devices tend to require a situation where the client is "thin" and the server is "fat": more tasks are delegated to the server, with the consequence that the server can observe more of the communication between the clients. For example, end-to-end encryption (more privacy preserving) might require more resources from the client than transport encryption (better for resource-constrained devices).

A server that has more control does not necessarily mean less privacy, as long as the users have control over the server. This happens when for example the server is run by an organisation and used by its employees, or when the organisation can be trusted. On the other hand, if the business model of the tool provider is (also) based on selling user data, then a server can be expected to perform in a privacy-invasive way (see for example past news on Zoom spying on its users). In any case, there is a possible privacy loss due to the introduction of a third party in the scenario.

Security is a dimension on its own, as it can not be categorised in terms of thin vs fat client or peer-to-peer vs centralised solutions. Security depends on the weakest part of the system, and each scenario has one (or more) potential shortcomings. As an example, peer-to-peer scenarios can be vulnerable if it is easy to impersonate one of the peers, and open source solutions like Jitsi can be vulnerable if the server running Jitsi is not secured and monitored. A high level of security (and privacy) requires to carefully examine each possible solution.

Several potentially conflicting characteristics emerge from the discussion presented so far. These characteristics can be used to examine a particular solution or design a new one. The importance of each dimension should be carefully considered as privileging one might imply penalising the others.