Future Urban Smartness:
Connectivity Zones with Disposable Identities

Authors: Rob van Kranenburg, Loretta Anania, Gaelle Le Gars, Marta Arniani, Delfina Fantini van Ditmar, Mantalena Kaili, and Petros Kavassalis

To provide citizen-focused empowering visions of smart cities planning and development is very much needed, especially when a post-COVID environment requires urban growth "resets" within stringent sustainability limits. Our selected case studies describe some of these current challenges. Two novel utopian visions of technology are proposed: urban "cold spots" and "disposable identities." The aim is to safeguard human digital rights in the digital smart urban sphere: our cherished freedom of expression, privacy, autonomy, and civic assembly. The chapter has three parts, the limits of smartness; the IoT, 5G, and 6G technology developments of cyber physical systems; and the need to choose a suitable form of identity management. Authors bring together their intradisciplinary approach.

Introduction

Our argument is on the limits of smartness, which concerns hyperconnected "hot spots". Smart use and a green transition suggest that we see "disposable identities" and minimal connectivity as a possible solution to mitigate a number of AI tracking and surveillance challenges. On the limits of smartness, we find that traditional smart city models may be useful for finite/quantifiable resources management (e.g., energy grids) and for providing specific services (e.g., parking meters). However, they fail in the face of anything encompassing citizen's collective behavior in an unknown context (e.g., terrorism, pandemics, environmental threats). Surveillance and data harvesting paradigms are exploding: prevalent, deployed ad hoc, often based on reproducing specific State powers or corporate interests. Control by means of AI based on machine learning models captures past patterns of collective behavior so as to predict the future.

This paradigm responds poorly to disruptive global events, either at macro level (e.g., the current COVID19 pandemic) or at a micro level prediction (e.g., an individual pedestrian crossing the street at the very last minute). We propose creating an urban "cold spot" to complement the 5/6G hotspot. Both spots are operated in the public municipality interest. We describe why and how they evolve. In part three we examine a series of case studies. Here the problem definition and odd context varies (fire, ship, art monastery). We look for commonality and differences, to fit the evolving urban context of AI, where connected IoT and cyber physical worlds coalesce: we call this a hybrid context. We find that disposable identities are a desirable implementation for the smart city residents.

Hotspots collect communication data and allow policy makers to investigate what it means to be human – including what it means to have human agency, diversity, uniqueness, and ethical choice. In future urban fully connected cyber physical systems, cold spots have a place. Both are needed to investigate new and old forms of mediation between humans and machines. Some of us functioned in a solely analogue environment. Urban cold spots allow for future alternative strategies of resilience in case of a breakdown of the technological infrastructure.

Whereas the hotspot is built on technical standards for the CPS/Internet of Things, cold spots are foreground for social trust standards in the Internet of People (Nold and van Kranenburg 2011). Cold zones would allow future urban residents a secluded period. An episode of digital interruption and think-time, more collective awareness and "suspension of disbelief" as psychologists call it. The gift of time and space is crucial and valuable, an almost lost feature of urban modernity and hyper-connectivity, with its restlessness and always on screen-addiction anxieties. Cold zones allow humans an increased awareness of the temporality of life on earth (a phenomenological, sensory, an experimental sand-boxing experience).

In addition to the On-Life initiative and H2020 Responsible Research and Innovation, the S + T + Arts (Science Technology and the Arts program of DG CNECT) links to our approach. The aim is urban regeneration through a creative space, open for technologists and artists to challenge the "status quo" and to stimulate others to perceive the new engineered realities.

Intelligent cities, information cities, ambient intelligence, and the design of cyber-physical systems for smart cities development have a long history of R&D (Droege 1997). Early design efforts were for the most part seen from an urban redevelopment and technology-push angle. Progress seemed inevitable, going hand-in-hand with urban growth and IT proliferation: demanding smart mobility, smart transport, smart working, automation, Internet connections and systems of IoT sensors-and-actuator systems embedded everywhere, 5G corridors, broadband access "anywhere any time," and so on. Studies show that frequency of human interaction relates to urbanization, mobile IT, and smartphone penetration. Then came crisis mode and climate change "reset." Urban residents find living in their cities a paradox, having the best and worst modernity to offer: access to services, transport culture, and the latest traded commodities, but also traffic jams, noise, deadly air pollution, cement-filled green areas, conglomerated expansion to the limit of planet resource sustainability. Cities are iconic, carrying a unique human-centered history. They grow as a place that attracts people, joining the affinity of those who were born or migrated there: residents that in collaboration can make it their home.

When humans and machines interact they communicate together and generate data. Cities need access to big data to visualize density of movement and patterns of social interaction in real time (big data visualization maps, information searches, Internet, and service monitoring). We focus our approach on a human desire for our space and time to follow a slower rhythm. The dream is an urban wellness commons: delimited cold zones for finding inner peace, social contact, and fulfillment. From the telecom angle, we need big data and small data, and can see density of urban movement in real time (e.g., big data maps), but also a desire for wellness zones for peace, social contact, fulfillment. We propose to characterize hot and cold zones in the table below.

Hot spots	Cold spots
Long-range digital value chain (telecom enabled)	Localized digital value chain (locally operating value chains for the needs of industry, services, and communities)
Opacity of local systems purpose, use, and beneficiaries	Transparency of local systems purpose, use, and beneficiaries
Social interactions mediated by tech by default	Social interactions leveraging tech intentionally when needed
Traceable presence	Anonymous presence
Individuals automatic categorization	Individuals self-determination
Privacy regulated at individual citizen level, accordingly to the policies of the devices she owns and the services she utilizes	Ambient privacy
Focused on quantifiable efficiency	Focused on Well-being
Density of tech sensorial/cognitive inputs (screens, sounds, vibrations)	Density of natural or social sensorial/cognitive inputs (grass, IRL interactions)
Top-down preestablished use of space and data	Open-ended use of space, data collectives
Commercial exploitation of aggregated data	No data collected

As urban 5G hot spots proliferate, a public debate extends from the car manufacturers, transport developers, and telecom manufacturers to everyone. The question is how service interoperability and systems can operate and cooperate in a shared data exchange and in what control context. Urban systems must operate in the public (municipality) interest. For instance, a city plan for serving nearby public research facilities, or event locations like a football stadium or concert/entertainment zones, business districts, or other entities operating with data trusts or as data collaboratives. Massive new investments are required for 5G to generate a return in business and research environments. Planned deployment of 5G should not just entail enabling everyone to download faster movies from anywhere on “best effort” old Internet connections.

The 5G districts can have hot spots, but we also envisage citizen support for greener "cold spots": circumscribed areas with low-range connectivity, low emission, less connectivity, more diverse benefits. The advantages are in consuming less energy, offering some autonomy and anonymity to explore surroundings with our own senses only, favoring possible reappearance of biodiverse spots or wilderness. Overall, in space and in time, we need less exposure to tech (screens, light, noise, waves, scanning). Cold spots provide valuable intervals of well-being and small wilderness protection.

We like the idea of disposable ephemeral yet verified digital IDs for cold zones. This solution is proposed as a timely alternative proposition for citizens living in the constantly connected mobile smartphone context of surveillance and data aggregation and proof of verified identity with every breath or digital step we take. Disposable identities and urban cold zones require collective willingness to trust others in sharing a new service infrastructure typical of the smart city. The following case studies explain how these possible solutions could work. The implementation of AI and cyber physical systems is rapidly growing, and we acknowledge the hybridity of these not-yet-mature yet deployed technology-push systems.

Reinstalling a level of social trust is essential to society as "polis." Local trust can be fostered by ensuring and respecting individual privacy, in a provable fashion, with auditable code, for security with far more transparency. The aim is to empower citizens to feel safer and more empowered online. In addition to the EU's GDPR, the twin transition brings in digital plus green governance and carbon emission "resets." All this will require stronger regulation. Regulators are standing in the midst of a global interac- tion level playing field, we are all players, we want a larger or smaller but definitely "open" access public space. Policy makers and institutional actors are required to adequately monitor, manage, and respond to resource crises in a timely and sustain- able manner. Managing a city means to acknowledge how hybrid today's context has become. As the world rapidly shifts from analogue to digital, rules, regulations, and infrastructures will coalesce like spaghetti on a plate.

A typical 5G case is to envisage the rules of engagement in an urban space of self-driving connected cars. The vehicles take decisions based on data streams that enable predictive analytics and many other forms of augmented decision-making processes. The data streams govern the car without necessary intervention and only a partial contextual knowledge of the human driver. Quality data becomes more important than territory presence as a means to stability and power.

Data and geo-surveillance in time and space is the new source of future value. The relationship between personal data and identity, including the associated agency, entitlement, accountability, and responsibility that goes with it becomes a strategic issue over the next decade. Back in the old analogue days the relationship between a person and a number was defined in one evidence of a constructed human reality with paper documents as material proofs (what actually happened, what one saw, what one did) under acquired norms and the rule of law system.

The hybrid world of today is more than that, it is data-augmented. It cannot just be the sum of analogue + the data stored and reprocessed in digital devices. As interconnected objects get their Ipv6 they become not only digitally addressable and traceable (item level tagging) but also collectors of data about people and the surroundings. Can the digital dimension rule over "the real thing"? The world of #IoT says "yes." Big Data, Machine Learning, and AI are no longer a technical features. Whoever owns knowledge of the relationships of these objects in the surroundings with one person's number can be a big brother. Currently companies with shareholder obligations and national governments with selected self-interests are given a large number of extra layers of capabilities and commercial applications not included in the original negotiated registration process nor democratically established and built with non- accountable (nontransparent algorithms). Such capabilities include a pro-active capacity, that is, predictions about behavior that are not fully shared – or only shared when beneficial to the country or company – with the person whose number is used. In the quantification of sensor input in the range of billions, Cyber Physical Systems (CPS) architectural layout of governance places humans alongside operators and (sub)systems in closed loop services. We argue that however valid this approach is from a cybernetic engineering perspective, we need a period of a deep human centered transition.

Disposable ID's enable a light form of governance in both hot and cold spots to investigate new forms of mediation between all the actors: people, services, operators, systems. As we will argue it is in this digital transition that the visible tools to point to the specific technological architecture disappears into the "fabric of everyday life." If the current 4G environment progresses "naturally" into a full 6G system of (cyber physical) systems, without any form of innovation or hot and cold spot experiments, fragmented 5G services will bring an unproductive trade-off in meaningful services versus perceived surveillance and control.

Part 1: Limits of Smartness

The overly optimistic and technocratic smart city narrative is experiencing a deep fracture. The parabola of Waterfront Toronto, from its launch in 2017 with the endorsement of Canadian Prime Minister Justin Trudeau to its demise in 2020 for "economic uncertainty due to Covid-19," encapsulates all the dysfunctions of the intelligent city: high costs; little capability to engage local authorities and citizens; opaque governance; concerns over privacy, data governance, and surveillance coming from the bottom-up as well as from global experts; concentration of value in the hands of big private players; little resilience in face of global disruptive events. The scale back of other symbolic smart city projects like Masdar City in Abu Dhabi and Songdo near Seoul testifies of a global negative trend. Besides the undoubtable economic factor of COVID-19, on a strategic level the recession of the smart city dream is caused by its incapacity to deal with citizens and uncertainty.

For the purpose of further research, the European Supervisory Authorities (ESAs) published a joint report (2019) on innovation facilitators (regulatory sandboxes and innovation hubs). The report sets out a comparative analysis of the innovation facilitators established to date within the EU and highlights the best practices. The extension of the concept of an innovation hub to the scale of a smart city requires the issues of governance and regulation to be adequately addressed. And while the regulatory sandbox is not yet a popular European practice, the standards of legitimacy of the development and function of a smart-city need to be addressed, holistically and extensively.

Gligoric et al. (2014) found that companies and services providers in the #IOT space barely recognized citizens in society at large as "users." Even when their contribution is crucial to a public objective, citizens' motivation and capability to use digital means is rarely taken into account. Singapore has gained recognition for making the source of its COVID19 TraceTogether app freely available to developers. Nevertheless, only 20% of the population downloaded the app and its role is therefore not clear. According to Marshall van Alstyne, business professor at Boston University, companies compete by adding new features to products, not building new mental models on how to add new communities or network effects. As the number of connected devices outnumbers humans, this may be logical from an engineering perspective (Gligoric et al. 2014).

The incapacity to deal with unexpected events has also a social determinism component. The smart city outlook into the future is based on algorithmic predictions that leverage historical data and imagine a linear and deterministic progression of events, with exceptions curbed out in a statistical model. There is a growing literature about how ADMS (Automated Decision-Making Systems) applied to social services reproduce bias and reduce consistently the opportunities for individuals' improvement of their socioeconomic situation, by tying them to their present disadvantage (Digital Future Society 2020).

At the crossing of citizens and uncertainty we find security. Crescent social justice concerns are voiced around the surveillance economy, or surveillance capitalism. They expose the failure of the current control system, which equates policing and governing. Within the criminal justice debate this is known as a spurious analogy since the 1990s: "police do not prevent crime" (Bayley 1994). Now that policing is augmented by technology and embedded as a public space feature, big tech is called to be accountable. Two American global tech companies, IBM and Microsoft, declared they will not support police departments with new Facial Recognition technology. IBM CEO, Arvind Krishna, highlighted that technology could get compromised in racial profiling and human rights abuse. Amazon instead halted law enforcement use of its facial recognition platform for 1 year. The limits of smartness in face of unexpected events are again present in the security world: being one of the most video-surveilled cities of Europe did not spare Nice from the 2016 attack on the Promenade (which preparation was filmed by city cameras ahead of the event). The ongoing debate in many countries about the privacy and security implications of social tracking in COVID-19 times has further foregrounded the debate from experts to a growing population of citizens.

Despite its lack of resilience, the traditional smart city model is likely to be revamped as an answer to COVID-19. The pandemic is already a Trojan horse for further surveillance, justified by the public interest. Anthony Townsend (2013), author of *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*, thinks the pandemic will accelerate the transition of Internet technology from screens to the physical world. This transition requires an adequate connectivity infrastructure. While the 5G debate is still heated, Samsung just presented its vision for 6G, which goes toward the direction of a blended reality: Immersive extended reality (XR); high-fidelity mobile hologram; and digital replicas. But 5G adoption already renders online vs. offline and infrastructure vs. applications binaries obsolete.

The implications for the current market structure and especially for the economic sus- tainability of TELCOS are at stake. Critical attention and suitable policies are important since the EU approach to 5G and 6G deployment relies on EU Telcos to drive the growth of an ecosystem conceived primarily to produce steady revenue streams for infrastructure operators. Jan-Peter Kleinhaus (2019) argues that if Huawei and ZTE were not Chinese companies, there would be no #5G debate: even after the Snowden revelations, there was no ban of Cisco equipment in European networks because of the trust in the US legal system and a mutually beneficial relationship. Still, Cisco owns around 60% of the global network switch market. Kleinhaus argues further "5G networks promise to expand bandwidth and add lightning fast data transfer speeds, which will allow billions of smart devices to communicate on the Internet of Things (IoT). But the IoT cloud will be built, essentially, on the broken architecture of today's internet, leading to an exponential increase in cybersecurity risks." The road to 6G is impervious, to say the least. 5G development is hampered by financing, regulations, cybersecurity, privacy concerns, high energy consumption, low adoption of supporting devices, criticality in land-scape interaction (dealing with real estate interests, planning the towers location), health concerns – evidence-supported, but also conspiracy-led.

The focus of EU digital policy, so far, is not deliberate about shaping the 6G paradigm. It is on the much narrower but more urgent problem of the strained physical limits on TELCO infrastructure. The EU, governments, and Telcos (Tele-com Operators) have all uncritically embraced the move to 5G, but the extent to which 5G will cause a reshaping of the market forces, or the implications for individuals, businesses, and society (i.e., multiplication of cyberthreaths with the increase of IoT-enabled objects), are not reflected in 6G policy stances.

Only in March 2020, with two EC Communications on AI and Data, the EU strategy has been expanded to include a more comprehensive approach to the ecosystem around the growth in data and connectivity which 5G will generate. In addition to 5G, the other main vector of systemic change ushering a radically different Next Generation Internet (NGI) will be the rolling out of digital identity schemes, across standards, management systems and related applications and environments. As it is complex and requires a denser coverage of base stations to provide the expected capacity, the cost of deploying 5G will be more than previous mobile technologies. According to European Commission estimates (2020), to reach the target, including 5G coverage in all urban areas, this cost is estimated at around €500 billion by 2025.

What is at stake is clear: to paraphrase Philip Alston (2019), avoid stumbling zombie-like into a digital surveillance dystopia. A dystopia that may not last long because of its toll on natural resources. We are facing the challenge of elaborating a novel urban operating system that is resilient to disruptive events because it is centered around its citizens and planetary wellness and based on equality.

While no unique alternative to the smart city as conceptualized so far is clearly articulated, most experts indicate that it should include higher degrees of privacy, as well as co-designed features: negotiated with citizens, also bottom-up approaches. By default identity should not always be detectable and citizens should participate to determine how they are to be identified by smart systems. The "smart enough city" as defined by Ben Green (2020) shifts focus from solutionism to the social needs that technology addresses. Similarly, the "responsive city" implies responsive citizens that use smart technology to contribute to planning, design, and management of their home cities. While such frameworks are desirable, we believe they act at an operational level: given a smart infrastructure and smart capabilities, the challenge is to acknowledge that the tech industry personas do not reflect the nuances of real people's identities – as exemplified by mistreatments of female, black, LGBTQ+, and low-income citizens, thus co-design with them better services. The number of connected devices will reach 500 billion by 2030, 59 times larger than the world population (8.5 billion by that time, according to Samsung (2020)). We argue that by the time the infrastructure is in place, it is already too late. Hence we took critics of the smart city to the limit, imagining a novel kind of urban space which infrastructure is from the ground up thought for its citizens.

Citizens are actors of smart city policies. Policies need to be constructed with citizens throughout the policy cycle (OECD 2019). As the digital divide is consistent, the digital skills-for-all policy should not lead to either "present" or "anonymous" as the default situation through anonymous ledgers but co-create through certified processes access to the benefits of the digitized city, and re-define the concept of fairness, accountability, and social interdependence.

Part 2: Zones of Connectivity

In the current governmental and commercial relationship frameworks, policy makers and enterprise architects deal with three main groups of actors:

- Citizens/end-users as individuals or crowds.
- Industry/SME and civil society NGOs.
- Governance/legal framework and established norms.

The data flow of IoT is a phenomenon that creates new demands. A central digital and interconnected feature is that the core identities of "people," "goods," "(legal) events" become fluid: interoperable and treated as properties, attributes, and/or credentials. We see a need to start to think again from basic building blocks. Starting with specific event-oriented identities that fit an urban regulatory environment, and setting a precondition that they be time-constrained.

Our propositional concept to grasp in this phase in the digital transition is the hybrid. Take a relative (semi) autonomous system view: the gaze of the network itself. This network is a mix of cloud and edge services (data storage resting on the smart device), with AI running inside objects in everyday activities (wearables, washing machines, cars). To this network all its users are "entities": machines, people, and processes. Each and all are templates of predefined scenarios. On the network "identity," as in singular identities, is no longer a relevant and productive concept, once removed of political, controlling, and marketing potentials. Liability-based models for insurance and indemnization in case of an accident with a self-driving car would reason as follows: the car gets awarded a temporary identity, the person(s) involved get awarded temporary identity, the rock the car hits before it goes into the water receives a temporary identity, as well as the (pollution in) water. The combined result is the "event" identity. It is a combination of these networked identities. On the basis of networked data tied to time-stamped identities liability, accountability and eventually some form of payment can be demanded or made. Event identities are combinations of real events, disposable identities, inferred behavior, and context from surrounding sources (cameras, sensors, wearables). The proactive scenarios can exist in virtual (non-embodied) analytics combined with AI capabilities can be enormous.

The main challenge in a democratic structure is to bring the governance of event identities under multistakeholder control. The challenge is to speed up quality decision making. Also, education, psychological frameworks, and new notions of "self" and identity can be developed (this has been termed understanding "what it means to be human?"). This development from the early Internet to the Internet of Things, our current 3G/4G world, is no fluke. Decision makers need to understand and be prepared for what the next iteration will be. The kind of connectivity it brings is known as pervasive computing (aka ubicomp, aka ambient intelligence). Computing disappears into the very *fabric of everyday life* (Mark Weiser 1991).

Cold Spots

The notion of public space has been progressively shrinking under the push of the data-extractive economy, as well as the equivalence of mass surveillance and security mainstreamed by 9/11 events. Since this extreme datafication of the everyday is driven by an instrumental approach to technology, which sees digital means as an extra layer of management capabilities on top of traditional ones, digital interfaces, and sensors have discretely blended into the urban every day. Although they may access the public space freely, citizens cannot tell whether they are directly or indirectly subject to any forms of data collection that will be either commercialized by third parties, or turned into machine-driven predictions influencing their life. We expect this opacity will lead to growing tensions in the coming years, with civil society movements claiming for more transparency and equality (e.g., Black Lives Matters, transgender rights groups) and municipalities formulating more clearly the relationship between surveillance and the public space (e.g., San Francisco banning facial recognition). Hence, cold spots are first and foremost a proposal to rethink the properties of public space in a hybrid scenario of humans and machines.

Cold spots are geographically delimited public areas. The cold zone digital infrastructure minimizes data collection and anonymises it through disposable identities. The infrastructure encodes a secure, public-owned open access regime. Hence, the "coldness" attribute derives from the lack of normalized data-extraction practices. From an urban planning point of view, the zones are seen as restorative areas (see below). They can be landscapes where nature is prevalent (parks, as well as "third landscapes" as Gilles Clément describes natural spaces of our cities that are yet to be encoded) or could be indoor areas (public libraries, recess spaces). Citizens can rest, wander, and organize collective activities. Security within the cold spot is not delegated to technology, but to municipal and national laws. Access to cold spots is regulated through the identity management described in part 3: if needed, the identity of the people present on site can be unveiled. This necessity has to be negotiated with all the stakeholders: the municipality, citizens, and any third parties (e.g., insurances in case of accident). In the coming years we aim to work on providing tools for this practice of mediation, the quality of which will decide quality of life. Further on, we describe four short cases that allow for this "switch" between hot and cold to hybrid.

By acknowledging the interconnection of social fractures and climate change, cold spots match key social properties of public space (i.e., mixity, interaction, sense of belonging) with the restorative ones of green spaces (i.e., mental and physical well-being, reducing emissions, biodiversity), on the background of a trusted technology infrastructure. They are novel urban wellness commons where city-making takes place. Creating a cold spot requires a blend of landscape interventions and digital policies that suits well the Horizon Europe mission of Sustainable Cities. We envision cold spots as areas that can be integrated in future urban planning as much as today we plan green areas.

Properties of Cold Spots

Restorative analogue and digital landscape. In landscape studies, the term restorative is used to explore the potential of outdoor settings in urban areas that can provide a general sensation of revival or renewal. Restorative means mitigating the stress and mental fatigue which can arise from prolonged exposure to some aspects of urban environments. Well before the information age, the metropolis was char- acterized as the place where people are overwhelmed by information that compete for their attention (Simmel 1984). Restorative areas provide experiences such as: "inducing reflective contemplative sensations; combining mental and physical worlds; offering conceptual escape, allowing the mind to wander; stimulating wonderment; being compatible with expectations" (San Juan, 2012). Their restorative potential emerges mainly from their capacity to facilitate social interaction and help induce contemplative psychological responses. Since the physical space is increasingly intertwined with the digital one, we argue that restoration in the hybrid novel setting should also include the planning of digital experiences within a given space. Cold spots are places for here-and-now experiences protected from datafication and surveillance capitalism.

Proximity Unplugged

Besides obvious sustainability reasons (i.e., limit emissions with a shorter supply chain), proximity is valuable for reinforcing the human social fabric, the creativity, and entrepreneurship of a specific city. Proposals emerging from different domains are reaching this same conclusion. To face COVID-19 disruption, the music live industry is formulating a new fruition model to go past the "low-cost flight + festival weekend" by investing in local scenes and talents, which are further connected globally (Grasmayer 2020). Similarly, the "15-minutes city" promised by Paris' mayor Anne Hildalgo bets on centering most of citizens' experience in hyper-localized universes within a 15-minute walk range (Euklidiadas 2020).

Fairbnb coop provides an alternative model to AirBnB by making short-term rentals financing local activities. We argue that cold spots are a key ally to any initiatives aiming at reinforcing localized but interconnected city-making. The big data value chain has a vast geographical spread: data can be collected in a given neighborhood, be stored in data centers in another continent, be used to operate systems at same-city level, inform decisions taken in the capital of the same country. Cities and citizens have little sovereignty on their data. Reducing the physical range of connectivity, cold spots are areas where value is not only produced, but regenerated and redistributed as an urban digital commons non-depletable resource.

Ambient Privacy

Ambient privacy is "the understanding that there is value in having our everyday interactions with one another remain outside the reach of monitoring, and that the small details of our daily lives should pass by unremembered" (Cegłowski 2019). The tensions emerging from the surveillance backlash expose the limits of the notion of privacy, framed historically as an individual right. We reached a stage where individuals cannot simply drop out of the surveillance society by refusing to use a certain technology or device: the whole infrastructure surrounding them is permeated by surveillance. Narratives of data ownership and consent are disempowering to the most: they shift the responsibility of a collective situation to the individual. Thus, we argue that to be truly empowering privacy needs to be collectivized and embedded in public space, infrastructured in its rules and functioning. We also argue that this geographical materialization of privacy can better serve sets of population that are suffering from inequalities in the exertion of their privacy rights (women historically, but also migrants or low-income citizens) through the feature of horizontal anonymity granted by disposable identities (Arniani 2020).

Wilderness

According to Arniani and Cazzaniga (2020) ambient privacy is strictly connected to wilderness, of which here we retain two qualities: the possibility of disappearing from the radar, and to build a deeper empathy with the beings encountered and to exercise presence. Cold spots are restorative pockets of wilderness within the city, landscapes that are integrated in the smart environment, but embed features, meanings, and values of the wild nature. Within them, the apparatus of cameras and sensors is absent, allowing again human spontaneity, mental and physical wonder. They can host soft infrastructures like hives, bird houses, and selected flowers and trees that can transform them in restorative areas for the urban fauna.

Trust

Imagining areas with no traceability challenges the equivalence of policing and governing: by delegating security to the use of technology, officials can avoid facing the complexities of the socioeconomic causes of insecurity. Within cold spots, trust replaces surveillance in guaranteeing security. As much as inhabitants of small cities sleep with their doors and cars open, cold spot regulars should feel the same amount of security. This is allowed by disposable identities. One should not imagine cold spots as the Wild West, but more as urban parks. They are regulated by municipal law: goers are liable for criminal activities. Identity data traceability is there, but just safeguarded from commercial interest and unauthorized use by the state.

Unprogrammability

Cold spots are opposed to the officiality of hot spots: while these are spaces where societal macro rules and history are encoded, cold spots offer citizens the possibility to perform the environment freely, according to their own micro-history and imagination.

This duality is the contemporary version of what De Certau (1984) was conceptualizing by distinguishing between strategies and tactics, a top-down city and a bottom-up one. Speaking of the second, he wrote "The networks of these moving, intersecting writings compose a manifold story that has neither author nor spectator, shaped out of fragments of trajectories and alterations of spaces: in relation to representations, it remains daily and indefinitely other" and also "they are not localized; it is rather that they spatialize." If space is hybrid, so is culture. For Homi K. Bhabha's (1996) theory of cultural hybridization "all forms of culture are continually in a process of hybridity."

Playfulness

Cold spots are areas allowing bottom-up experimentation. In this, they resemble maker spaces and artistic residencies in their capacity of making available spaces, tools, ideal conditions for thought, and concentration. They can host citizen science projects, spontaneously organized courses, rehearsals, or entire performances.

Value Proposition

The "value proposition" of cold spots is to:

- Improve citizens' well-being, especially mental, with a well-situated publicly owned, transparently managed, and noncommercial space for mindfulness and presence.
- Foster localized creativity and innovation – in culture and creative forms of artistic entrepreneurship, to then make use of digital means to operate or scale. Creativity as a collective endeavor is possible with face-to-face encounters and a vibrant local cultural milieu.
- Increase trust in public infrastructures, strengthening openness, both transparency and anonymity.
- Low energy consumption and low carbon emissions by advanced (green, blue) technology infrastructure.
- Support for biodiversity, reduced noise, and light pollution.

Play

We imagine cold spots as a network of areas, overlapping but not only, with green areas. We argue that cold spots can better counterbalance the pervasiveness of traditional connectivity and distribute wellness if they are widespread across the city. In the Sixties, Robert Zion dared to propose a network of vest pocket green areas scattered around the city, with the role to ease the metropolis stress along the normal everyday routes of city dwellers. At the time, Central Park was the peak of innovation. Similarly, we believe that the solution to urban fatigue and lack of sustainability is not in the choice between over-connected and disconnected zones, but in distributing cold spots as areas that leverage technology innovation in a human-centric way. In this, existing urban green areas are an ideal ground for pilots. Here we picture the role of a "cold spot park" in facing pandemics, as an extreme case of both physical constriction and technology-led surveillance. With the current pandemic expected to last at least 18 months and possibly new ones on the horizon, it is urgent to rethink the balance between applying strict measures and allowing social and cultural life.

Pre-COVID-19, the demand for offline mental concentration was spiking, with the proliferation of mindfulness apps, site-blockers, Internet-free exotic luxury retreats, wealthy digital tycoons sending their children to tech-free schools (Weller 2018). The disorganized digitalization of many face-to-face activities following COVID-19 has increased mental exhaustion to an extent that novel terms are needed to describe it (i.e., "Zoom fatigue"). In times of pandemics cold spot parks are areas that democratize well-being because not only they provide an open outdoor space that counterbalances the narrowness of home-work and home-schooling but also they provide a restful pause from the overexposure to technology and constant traceability at walking distance.

They reduce the possibility of contagion without shrinking social and cultural life, the great victims of COVID-19 measures: they allow both physical distancing and social interactions under an anonymity shield that can be promptly lifted if a contagious person is found to have hung out in space. The trustable digital infrastructure makes contact tracing apps useless within the cold spot, because the tracing of the virus is collectivized along the ambient privacy principles. This resolves the enormous problems of adoption that these apps experience across the world in democratic societies.

When they enter a cold spot park during a pandemic, citizens know that their individual identity is unknown and their movements free of tracking. At the same time, they feel protected because they know that they will be alerted if they were close to a contagious person. They feel alive and empowered, because the cold spot gives them room for cultural activities, interactions outside their co-habitants circle, and physical activities.

We need a Trust-Framework to safeguard constitutional values, the notion of an inclusive society and a focus on equality. According to Manon den Dunnen who works at the Dutch Police as a strategic specialist on digital transformation, there are three main issues involved: control over your personal data, availability of data for social goals, cheaper data exchange as it is costly and inefficient. The current way of data exchange is complex and inefficient. Every provider of digital services has to arrange for the identification, permissions, and logging of transactions themselves (NGI Thingscon 2019).

The Trust Infrastructure consists of a generic facility providing core services like identification, authentication, consent, and security. Next to this, it consists of data collaboratives that ensure responsibly functioning data markets. These organizations develop data sharing agreements, draft related consents agreements and manage the granted permissions. For the verification of identities and data-sharing permissions, these organizations use the generic provisions of the DVI. The incentive to do so is that it allows them to access data in a GDPR-compliant, low cost and easy, accessible way. In return, they must meet the requirements in terms of transparency and privacy and security by design.

As an example of the added value of data and the importance of a Trust Framework she introduces Jannie. She lives in an apartment complex, has difficulty walking, and sleeps with an *oxygen bottle*. The neighbor on number 38 down the street has her spare key. Normally nobody has anything to do with that, but if there is a fire, then it is very important for both Jannie and the fire brigade that this information is known. So how do you ensure that this information is only visible to the fire brigade and only if there is a real fire, without all other personal, medical information being disclosed? In short it is about:

Who may do what with my information under what condition and to what purpose? This seems simple, but there is quite a lot involved, such as how do you know for sure that it really are Jannie and the fire department, or that Jannie still lives there? In addition, it is impracticable and undesirable that the fire brigade makes 1 on 1 agreements with all residents. Then register all this and carry out checks.

In the example of Jannie, a 112-alert App is created for which you can register and in which you can indicate which data you want to share. The great thing about this solution is that anyone who wants to can participate, but it is not necessary. It is not known to the fire department who does or does not participate, so there is no pressure. In addition, everything is logged, so that it can be checked transparently. The DVI does not contain any data, it only checks the permissions and conditions after which the two parties can exchange data with each other.

In this pilot the default is the cold spot, the house is calm and unsurveilled. Yet, in the case of a fire, in this case a clear and present danger, the house turns into a hotspot, disclosing information to carefully chosen service providers.

Art of Smart

> "*If you want to understand what's most important to a society, don't examine its art or literature, simply look at its biggest buildings.*"— *Joseph Campbell*

Creative fora and cultural institutions are not optional for a truly smart city; they are implicit of any concept of community and resilience. Not only art has always served as an accelerator and messenger to a more general audience of new ideas, but its main role is to maintain human in the epicenter of innovation.

In the context of the European program S + T + Arts Regional Centers in Greece, the nonprofit platform MADE GROUP, with the support of the Cultural Association of Archilochus, sets the foundations for future collaborations in Paros, the Island of the whitest marble in antiquity. Within the scope of the S + T + Arts program, where the transdisciplinarity and combination of science, technology, and art practices and knowledge aim to create opportunities for synergies and social progress, the project Random Rhetoric assembles democracy with Epicurus' swerve (παραΕκκλιση parénklisis; Latin: clinamen), an idea that describes the slight deviation and randomness of atoms from their "ordinary" pathways. The artist and professor Yiannis Melanitis works on democracy refers to a geometrization of the art of oratory and its processes through the randomization of information: "Political speech and philosophy emerging from machines and computers render humans to mere 'viewers' or envisage new roles in society." He anticipates that "even the official state structures of future dialectics may be derived from self-programming computers."

In the Random Rhetoric digital forum, "a computer is programmed to answer and interact in dialectics about the role of citizens in a republic. Audience might notice that this interaction opens up a thinking procedure unexpected and random, but still logical (all sentences are logical, even if their rows might be more complex). There is no face, body or other presence sign of the orator except sound. An orator presupposes to be on a stand, a BEMA (βήμα, bima, the podium). Instead of a BEMA, I use a negative BEMA structure, a reversed model. A reversed speech order also is active in the work: you might think you respond to a machine that thinks, but it has been structured to trick humans" (Melanitis 2019).

Without an embodied human perspective and a social context AI as a speaker of "data/truth" is as devoid of meaning as speech itself in the perspective of Aristotle on rhetoric: "Rhetoric is a sort of division or likeness of Dialectic, since neither of them is a science that deals with the nature of any definite subject, but they are merely faculties of furnishing arguments" (Aristotle, Rhetoric, 1355b–1356a). Works like this we regard as important tools for awareness and ultimately negotiation for stakeholders to decide when situations become "emergencies" and whether then switches from hot spots to cold spots and vice versa may occur.

The foundation of the digital transition is profoundly not neutral. Take the act of naming the entities at the lowest level: "In reasoning about the relationship of words and objects, Antiphon, the Attic Orator, makes a unique conception, that nothing real corresponds to the name of an object, leaving onomatology in the realm of pure chance, while true knowledge becomes inaccessible. Name correctness becomes a key point for Antiphon and should be under survey: Names can be erroneous. The concepts we use are not delimited by the exact way objects are." In building cybernetic models of decision making it remains fundamental to remind the computer architects and engineers that even at the lowest level there is no vital or inevitable correlation, and each and every decision can be contested as non-neutral and political.

Hot Spots

The closest attempt to instantiate a hot spot is a "6G CPS hub," where CPS stands for cyber-physical systems, and 6G – the successor to 5G – is significantly faster, at speeds of ~95 GHz. CPSs are engineered systems "integrating information technologies, real-time control subsystems, physical components, and human operators in order to influence physical processes by means of cooperative and (semi)automated control functions. key features of CPSs are:

- (1) real-time feedback control of physical processes through sensors and actuators;
- (2) cooperative control among networked subsystems; and
- (3) a threshold of automation level where computers close the feedback control loops in (semi)automated tasks, possibly allowing human control in certain cases." (Guzman et al. 2019)

The human is seen as an integrated human "operator," alongside components and subsystems, into an ultimate decision-making feedback control loop in which human control is allowed "in certain cases." Research into the mental models that foster this ability to be integrated is studied with regard to psychophysiology: "Biomechanical integration involves ensuring that the system to be used is ergonomically acceptable and 'user cooperative.' Psycho-physiological integration involves recording and controlling a patient's physiological reactions so that the patient receives appropriate stimuli and is challenged in a moderate but engaging way without causing undue stress or harm" (Koenig and Riener 2016). This procedural operation works both ways. Google developed Cloud AutoML in order to train machine learning models with minimal human expertise. AutoML-Zero requires even less human involvement. Intertwined with CPS is the notion of the Digital Twin (DT) as both a prerequisite (in order to digitally twin every conceivable unit or item), and "a comprehensive physical and functional description of a component, product, or system" (Taoa et al. 2019). In "Cyber Situational Awareness for CPS, 5G and IoT," by Elizabeth Chang, Florian Gottwalt, and Yong Zhang, the authors claim that as the wireless future is mobile "the 2020 wireless strategy is centred on creative 5G and IoT with the front runners from US, EU, China, Japan and Korea" (Yang 2018).

Whose digital world is this going to be? It is this novel paradigm, cyber-physical-social systems (CPSS), fundamentally altering the relationship between humans, computers, and the physical environment. That needs new forms of governance toward the 6G hotspot roadmap. Apparently 5G and CPS are two sides of the same coin, yet its fragmentation will not be solved alongside the development path. That is why the 6G roadmap should work back from a novel governance structure.

Deployment of 5G makes it easy to transport data to the cloud, to make predictions and models faster. Telecom providers put the emphasis on enhancing consumers' devices, giving for granted that the infrastructure will be operated as the old Internet: as much ubiquitous and invisible as possible. Sanyogita Shamsunder, Verizon's vice president of 5G Labs and Innovation. says: "wearables will be able to send and receive far greater amounts of data wirelessly, providing the people wearing them with vastly more digital information." Smart earbuds, or "hearables," provide information via audio including directions that can be heard only by the people wearing them. Nearly a dozen companies sell smart glasses aimed at health care, "exercise enthusiasts, music aficionados, and owners of smartphones with no headphone jacks" (Alsever 2020). The RIQ News Desk in 5G on Wearables Set to Disrupt Mobility wonders if "today's uber-tool," the smartphone, will stand as the next carriers may turn out to be smarter, the combination of 5G and wearables could make the smartphone revolution seem like a miniscule advancement.

The latency of about 1 millisecond coupled with the high reliability of the network will enable a very high degree of real-time control – and this instantaneous and on-the-go attribute is what makes the content experience for –wearables so user-impressive (RIQ News 2020). Future 5G antennas for wearable application will be "compact, low-profile, comfortable and feature mechanical robustness, insensitivity to changes in user movements and robustness to deformations, varying mounting locations and body morphologies" (Aun et al. 2017). This means that information on the device can be stored throughout its lifetime (edge) and shared at specific moments with dedicated clouds to complete the security of the system which would operate in a closed-loop.

The benefits for citizens is that instead of a client (which can be a person or a connected object) actively pulling for data and information, the data, information, and services get pushed to clients that expose their wants and needs in a coherent way. This represents the shift from Customer Relation Management and search engines to Vendor Relation Management (VRM). VRM gives customers means to relate to many different companies, institutions, governments, and citizens. According to Doc Searls: VRM is the "logical business process that complements the Internet's end to end architecture allowing business to take advantage of full participation with customers.

Once customers can become true partners with the companies they engage, the economic upsides become incalculable, because clear signalling will be maximized in both directions. Simply put, free customers will prove more valuable than captive ones" (Searls 2012).

One is tempted to say that the benefits for "the system" is having a control dashboard: the most counted words (over 20) in "The New Geopolitics of Converging Risks: The UN and Prevention in the Era of AI," United Nations University Centre for Policy Research are "inclusive foresight" (inclusive horizon scanning): "An inclusive foresight tool, housed at the UN and shared across key stakeholders, can be the locus for 'preventive innovation,' offering new opportunities for stability and security worldwide" (Pauwels 2019). Yet conceptually we are faced with the fact that in this CPS hub/hot spot we can no longer distinguish between the "system," the "person," "services," "operators," "robots," "machines" any more so we need a new vocabulary to even think as ourselves (are we still "there"?) in a governance framework, and a new notion of identity becomes paramount as the former fixed categories (people, goods, machines, operators, subsystems, etc.) become fluid and interdependent.

In this light, it is not just regulation, contested issues, cost, spectrum issues that are "hampering" 5G uptake. Many use cases of connected cars, such as smart mining, smart port, smart manufacturing, telemedicine, immersive experiences (AR/VR) cannot yet show added value, whether for consumer or business, as long as they are not integrated into a CPS hub as that "contributes a set of very essential technical enablers – including virtual power plants, and interaction within day ahead/intraday energy markets – for future smart CPS systems and creates a strong basis for such future research towards a future smart society" (Latvakoski and Heikkinen 2019). Without a strong policy vision on 6G, 5G might not deliver the promised digital integration of services and applications.

The six services citizens indicated they were willing to pay for in the 2020 Capgemini Research Institute Report are basic elements in the hotspot:

- Automated connectivity of buildings to emergency services.
- Remote patient monitoring for older citizens.
- Smart home energy consumption tracking.
- Centralized building energy automation systems to control hearing, ventilation, and AC.
- Smart card of app-based access to public transport.
- Real-time water quality monitoring (Capgemini 2020).

Enterprise architects and experts to policy makers can now make the following conceptual model. If 5G sets forth as well as requires CPS, the notion, concept, and actual embodied human acquires a new status alongside operators, material elements, and subsystems:

> An intelligent unit is the smallest functional unit of intelligent manufacturing. It comprises humans, cyber systems, and physical systems. An intelligent system integrates multiple intelligent units through the industrial network to achieve automated data flow in a larger scope and across broader areas. It helps to improve the breadth, accuracy, and depth of manufacturing resource allocation across production lines, workshops, and businesses to form a system-level HCPS. An intelligent SoS is a system that integrates multiple intelligent systems through Industrial-Internet-based integration across systems and platforms. It cre- ates an open, coordinated, and shared industrial ecosystem, thus forming an SoS-level HCPS. (Zhou et al. 2019).

It is tempting to reflect upon this from a position of loss of human agency, but it is our architectural duty to investigate what can be gained in this development, not embrace it as in a transhumanist position somehow longing for the intermingling of these elements, but investigate it with a critically positive mindset.

CPS might help us to deal with the trust fallacy, that is, as if a precondition to "trust" exists, that is, as if a position exists that can be matched, fulfilled, checked. That position is always empty, temporarily occupied by force by an arbitrary issuer of "trust," acting as if it were a product that could be made, achieved, bought, or sold. In CPS this primordial position is open, foregrounding as a key to identity not trust, but *conflict*. If the basis is conflict, always in process, in motion, moving, instead of trust as a potential given, at rest, then we must conclude there is no *intent,* no intention, as this precedes this perceived position of trust. We have built (k)institutional practices and the very notion of the well-rounded personality as a core of identity seeking trustworthy relations on intent, that is conscious and thus account- able actions and activities. In fact, it seems that we need *intent*-as-a-concept to model accountability (blame and shame). This modeling has enabled us to penalize individual acts and exonerate large-scale effects of behavior like environmental damage leading up to Climate Change and social extraction of resources to inequality, poverty, and dissent. If intent is linked to an incorrect assessment of identity, and thus not central to an ethics of behavior, then this opens up an actionable set of actors actually at play in the CPS hub namely: objects (with added connectivity like NFC), machines with built-in connectivity, animals and plants (as ecosystems), and humans alike, as they can be treated as *entities*.

This allows us to focus on the interplay of entities and its effects on the full ecosystem. Moreover, this allows us to build new enablers for governance tuned to a real understanding of twenty-first-century technology, its powers and its drawbacks. It enables us to stay fully human, yet abdicate from the primary position of meaning maker based on a presupposed feature that we somehow should have and other actors lack – intent. It enables us to build 6G CPS governance for AI, Machine Learning, 5G, and IoT as we can expand the notion of citizenship and identities tied to passports and social security numbers of people into an ecology of identifiers that have entities at its core.

The Cruise and Passenger ships Hybrid-Spots

In the case of advanced connectivity services provided for people safety purposes and other specific reasons (such as the provision of location-based services) an advanced connectivity spot may alternate between "hot" and "cold" statuses. A "coldspot," for example, can turn to a hotspot in the case of an emergency or become a "hotspot" for a particular user if she/he needs to temporally access specific location-based services (health, e-commerce indoor object search etc.).

A cruise and passenger ship provides such a case which requires the re-assignment of advanced connectivity resources and the dynamic deployment of the policy rules for privacy when an evacuation plan is launched. In this context, a generic mechanism for crew and passengers indoor positioning. Indoor Positioning Systems (IPS) can use 5G core functionality to locate with precision the position of people within interior spaces, in complex buildings (factories and offices), parking garages and underground constructions, alleys, shopping malls, airports, etc. –5G-enabled IPS systems become a critical part of a new generation of (smart) evacuation management systems deployed in cruise ships and RoPax vessels which combine advanced passenger traceability with operations management capabilities (i.e., providing directions in real-time to and through the evacuation paths and crowd monitoring). If an evacuation hindering incident is reported, these advanced services monitor the evacuation process through high accuracy people tracking, observation of passengers toward the mustering stations, counting and analytics. And, assist SAR (Search and Rescue) dispatched forces to search and find survivors and approach them.

Advanced connectivity services with dynamic indoor-positioning capabilities can be designed to act in real conditions to deal with hazard upon its occurrence by using a reactive approach: in normal times, they will be allowed to run on a minimal function mode providing "coldspot" mù- functionality; they will be activated when an irregular situation is detected and become fully functional "hotspots" under the administration of the bridge.

Similarly, a passenger herself can alternate the service functionality and enjoy indoor navigation within a large complex ship, additional security safeguards, or location-based entertainment service. The networks providing these alternate between cold-and hotspots will not be operated by telecom providers but are deployed on specific service environments as independent peripheral networks by service providers and local communities, based on governance rules that should be accepted by the user before joining the service network.

Part Three: Disposable Identities

The notion of a cyborg world was apparently coined before the year 2000, from work by the US National Science Foundation. It has become part of popular culture since. As a blueprint for the future urban environment it is quite limited. The temptation is to conceive of a smart machine world where humans stand on the side, losing agency and eventually their old values, as cyber physical systems become indistinguishable from life. A very old science fiction idea that with AI is gaining more traction; as blueprint for the future digital environment, much of it not, of course, consciously embraced by those who contribute to the design of the new control systems and internets, but it is in this context that digital identity is being developed right now.

Disposable identities act as an e-ID that can ensure both the anonymity of the identity owner and the possibility of reliably identifying and verifying a person's identity. Naturally, cold spots may offer to their users the opportunity to navigate through content and services by using disposable identities attributes – hotspots also can also support and incorporate the use of disposable identities in the provision of services with high privacy safeguards requirements (e.g., in the case of a citizen accessing online health application). We assume the existence of hybrid forms between hot and cold spots, that is, hot spots that can provide high privacy safeguards in the access of online services. .

As explained before, cold spots would allow citizens to navigate and live safely without necessarily revealing their complete identity while ensuring their movements are free of tracking. Disposable identities is the key enabler for creating an environment strongly and a priori reducing exposure to privacy-invasion and freeing up participants from the paralyzing effect of privacy-related fears.

The Financial Action Task Force (FATF) defines an "official identity" as the specification of a unique natural person that is a) based on characteristics (attributes or identifiers) of the person that establish a person's uniqueness in the population or particular context(s) and, b) recognized by the state for regulatory and other official purposes. In fact, virtual "green spaces" should enable the creation and stimulate the use of a specific form of minimalistic identity that is "official" in the sense of FATF but based on a digital certificate that exists only temporarily and in the specific context of a cold post-hosted online activity – and structurally "unlinkable" to personal, formal, identity information (PII data or mobile ID). We have elsewhere call this minimalistic, context-specific and time-limited identity a safeguarded, or disposable-yet-official identity (Anania, forthcoming). It is essentially a policy framework and technology toolbox we should adopt to balance between certainty (i.e., identity verification accompanied by strong privacy-preserving policies based on normative boundaries for the processing of personal information) and flexibility (i.e., the utility we receive from the digital use of identity information which includes privacy statements that are cryptographically enforced).

Disposable identities is a further step toward minimal data processing: the amount of identity data processed should be adequate, relevant, and limited to what is necessary for the purposes, as it is required by the GDPR regulation, Disposable identities are temporary attribute-based identities integrated in a smart contract (in the large definition of the term) between a receiver and a supplier of a service. Enabled by a Self-Sovereign Identity (SSI) architecture disposable identities are capable of providing anonymized, near real time, tamper free, and verifiable identity information. This is mainly achieved using Disposable Yet Official Identities (DYOIs), a model of Disposable Identities based on SSI architecture and adopting the principle of (unlinkable) DIDs over which a person has ownership or control.

Self-sovereign identity (SSI) recognizes an individual should own and control their identity without administrative authorities. Through SSI people can interact in both the offline as the digital world with the same capacity for trust. It operates trustworthiness through "verifiable credential (a set of claims) created by an issuer about a subject—a person, group, or thing— ... presentation of proofs by the bearer; data minimization; and centralized, federated, and decentralized registry and identity systems" (W3C 2020). Disposable Yet Official Identities mean that:

- They can be issued by an official authority, but they are completely managed by the identity subject through a mobile wallet application, and stored in the citizens' mobile phones in an encrypted form.
- They can include accurate (official) personal information, contain proximity data or anonymized GPS location data, but they are structurally "unlinkable" to the subject's personal (official) identity information (PII data or mobile ID).

In other terms, a Disposable Identity is made from service or domain specific personal data and allows the subject to prove ownership over these data, without permitting anybody else to make (present or future) correlations between them and the subject's true identity. Essentially, a subject for navigating within cold spots can generate many purpose-oriented "disposable" credentials, which are linked to different DIDs over which a person has ownership or control. The term Decentralized Identifier (DID) is used to describe an identifier that is publically discoverable using for example a distributed ledger. However, the public nature of a DID should not be mistaken for a potential user tracing enabler. Indeed, user DIDs need not disclose anything more than endpoints and cryptographic public keys. Only the subject themselves can make the correlation between the different DID under their ownership (unlinkability).

Furthermore, a Disposable Identity (or, better, a disposable proof of identity) should point somehow to an "Official Identity" and in that way is distinct from broader concepts of personal and social identity that may be relevant for unofficial purposes (e.g., unregulated commercial or social, peer-to-peer interactions in person or on the Internet). In other terms, there is always a possibility to align a Disposable Proof of Identity (DPI) to an official identity; if requested, a disposable proof of identity can be explicitly linked to an Official Identity (National ID, eIDAS eID, Online Passport) via a "Verifiable Presentation."

A Verifiable Presentation links the attributes of a Disposable Identity to the attributes of an Official Identity, that means validates an identity presentation while ensuring anonymity (e.g., it can prove that a person presenting a disposable identity proof is, in fact, a real natural person under EU/national law or the representative of a legal person). Further, it integrates attributes from different identities to a joint "Verifiable Presentation." An example: a ticket for a local cultural event (essentially, a right granted to a user that allows her to enter such an event, a concert or a festival) is linked to person X' "official" identity attributes [name, surname, uniqueID]. But the "linking" is not provided by a Service; only the Subject, if requested, can create and present links between different Disposable Identities, or between a Disposable and an Official Identity.

From a technical point of view, Disposable Identities are Verifiable Credentials (VCs), in the sense of W3C Consortium (Wang and De Filippi 2020). A Verifiable Credential, that is, an identity statement made by an Issuer about a Subject, is capable of representing all of the information that a physical credential contains, but additionally is tamper-evident and more trustworthy than a physical credential since it can be cryptographically verified. Further, DIDs are used to identify the Holders (subjects) and the different VC Custodians, the Issuers, and the Consumers (Verifiers) of Verifiable Credentials

A subject can generate many purpose-oriented "disposable" Verifiable Credentials (Disposable Proofs of Identity) which are linked to different DIDs over which a person has ownership or control. Using Pairwise DIDs or Peer DIDs, subjects are able to generate new DIDs, on the fly, and securely and privately communicate with a party making correlations with other parties effectively impossible, thus implementing a privacy-by-design property.

- Only the subject themselves can make the correlation between the different DID under their ownership (unlinkability).
- The combination of Pairwise/Peer DIDs together with Verifiable Presentations based on ZKPs (Zero-Knowledge-Proofs) provides a sound foundation for a system that prohibits the tracing of the subjects' actions and provides technological safeguards that exclude any possibility of linking DID data (unlinkability), and effectively dissuades a possible collusion between the different parties of the system.

Example: Alberto, generates a DID (say DID1) to interact with some authority, VCissuer1, to create a Disposable Proof of Identity, DPI1. Next, in order for Alberto to prove to a Service Provider (SPk) that he is in possession of some attribute, Att1, contained in DP1, Alberto generates for SPk a new DID, DID2, so that he can initiate secure (SSI standards-based) communication with SPk. DID 1 is in no way derivable from DID2. So there is no way for SPk and VCissuer1 to collude and trace Alberto's actions. Then, Alberto generates a Verifiable Presentation consisting of a Zero Knowledge Proof (ZKP). This proof allows Alberto to prove to SPk, irrefutably, that he is in possession of DP1, signed by VCissuer1, that contains Att1. This proof again leaks no information about the actual DPI1 or the identifiers contained therein. It just allows for SPk to verify that Alberto is indeed in possession of this attribute.

Conclusion

Mark Weiser, in his 1991 text *Computer for the twenty-first Century*, explains the fundamental nature of the shift by demonstrating that the success of ubicomp (the term in the 90s for #IoT) is its full disappearance as visible technology in the "fabric of everyday life." If we think of governance and technology throughout the ages as foregrounding agency on the tools that were tuned to visible interfaces, it becomes clear how important it is to fully grasp this disappearing moment. For where is the handle to the door? The knob on leveling sound, power, speed on the machine? The cursor on the screen that guides you through virtual data-sets? What happens ontologically to an architectural position if it can no longer distinguish between the analogue or the virtual Digital Twin? This disappearing into the fabric of everyday life is the single most important generational moment of the early twenty-first century concerning the notion of identity as the basic and "essential" unit to ground political, architectural, and operational agency; firmy ending the Renaissance paradigm that "discovered" (through Rousseau) the "individual" as the basic element for a political ethics and praxis.

This process is the deep driver behind a set of seemingly unrelated but coherent emerging practices: the empty essence that was temporarily filled by the notion of the psychologically "whole," administratively numbered (social security, passport, telephone, etc.), socioeconomically responsible, and ethically accountable "person" is shifting from "occupied" to "empty" again rendering all the tools operating at any of these levels gradually more impotent. The agency on any level (architectural, ethical/moral, economic, well-being, politics, etc.) is shifting to the level below: the set of attributes, properties, characteristics credentials, which we discussed as *event identities* in part 2.

In the last 5 years, the notion of a Self Sovereign Identity (SSI) has emerged. The notion of citizens evolving from surf-hood to sovereigns of their data and their identity goes well with the European mindset of unity in diversity. The Union and its treaties was conceived not with member states but with citizens as the main actor: Article 3 (e.g., Article 2 TEU). "The Union shall offer its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime" (Treaty, 2007). The disposable identity concept is perfectly aligned with The General Data Protection Regulation 2016/679, the regulation in EU law on data protection and privacy in the European Union and the European Economic Area.

We construe digital identity as relevant for governance in both hot and cold spots. Disposable IDs can leverage the infrastructure of hot spots, and most importantly, the sociopolitical consequences of surveillance capitalism, yet acknowledging the hybridity of the system and reinstalling a level of trust. They allow citizens to feel safe when they are asked to use tech in the public interest and they allow a more suitable management of the "unknown" and a better response to it. The citizens are given the option and the access, both essential elements for a balanced community.

References

Alsever, J. (2020). With 5G, wearable devices are expected to become even more sci-fi. Tech section Fortune. *Newsletter* https://fortune.com/2020/03/24/5g-wearable-devices/ Accessed 10 August 2020.

Alston, P. (2019). *World stumbling zombie-like into a digital welfare dystopia, warns UN human rights expert*. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx? NewsID 25156 Accessed 10⁄4August 2020.

Alvarez, Towards Gender Equality in Digital Welfare, (2020) Accessed 10 August 2020 Gender equality strategy 2020–2024. Just D2 https://ec.europa.eu/info/policies/justice-and-fundamen tal-rights/gender- equality.

Anania, L., van Kranenburg R., & Le Gars, G. (2020). Disposable Identities? Why digital identity matters to blockchain disintermediation and for society (forthcoming). In D. Psarrakis & E. Kaili (Eds.), *Disintermediation Economics: Markets, Policies, and Blockchain* Palgrave Macmillan: New York .See also: Kavassalis, P., Triantafyllou, N., Georgakopoulos, P., Stasis, A., van Kranenburg, R. (2020). Lessons from the event COVID-19 health crisis: The case of digital document verification and credential-based access control in ad hoc outdoor and indoor settings (and beyond) using safeguarded identities, Working Document, University of the Aegean.

Arniani, M. & Cazzaniga, G. (2020). *Media Architecture Biennale Workshop Proposal: Planning Restorative Areas of Urban Wilderness Through Ambient* Privacy https://mab20.mediaarch itecture.org Accessed 10 August 2020.

Arniani, M., Digital Future Society. (2020). *Towards gender equality in digital welfare*. Barcelona, Spain.

Aun, N. F. M., Soh, P. J., Al-Hadi, A. A., Jamlos, M. F., Vandenbosch, G. A. E., & Schreurs, D. (2017). Revolutionizing wearables for 5G: 5G technologies: Recent developments and future perspectives for wearable devices and antennas. *IEEE Microwave Magazine, 18*(3), 108–124. https://doi.org/10.1109/MMM.2017.2664019.

Bayley, D. H. (1994). *Police for the future (studies in crime and public policy)*. New York: Oxford University Press.

Bhabha, H. K. (1996). *Cultures in between. Questions of cultural identity*. S. Hall and P. Du Gay. London, Sage Publications.

Cegłowski, M. (2019). *The New Wilderness*. Idle Words blog. https://idlewords.com/2019/06/the_ new_wilderness.htm Accessed 10 August 2020.

Combs, V. (2020). 6 smart city services people would pay for and use. In: Digital Transformation. Capgemini Research Institute – Street smart: Putting the citizen at the center of smart city initiatives. https://www.capgemini.com/research/street-smart/Accessed 10 August 2020.

Consolidated version of the Treaty on European Union. (2007). Protocols – Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon. Official Journal C 326, 26/10/2012 P. 0001-0390.https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012M%2FTXT

de Certeau, M. (1984). *The practice of everyday life*. Berkeley: University of California Press.
Droege, P., editor (1997). *Intelligent environments: Spatial aspects of the information revolution*.

North Holland publishers, Elsevier. Intelligent Cities, ACMÂ iCities publication, Germaine Halegoua, MIT Press 2020.

Euklidiadas, M. M. (2020). Paris wants to become a "15-minute city". *Tomorrow City Magazine*. https://www.smartcitylab.com/blog/governance-finance/paris-15-minute-city/Accessed 10 August 2020.

Gligoric, N., van Kranenburg, et al. (2014). Making Onlife Principles into Actionable Guidelines for Smart City Frameworks and #IOT Policies. In *Designing, developing, and facilitating smart cities urban design to IoT solutions* (pp. 33–49) Springer.

Grasmayer, B. (2020). Why local is the answer to a future of new normals. *Newsletter*. https://www.musicxtechxfuture.com/2020/08/04/why-local-is-the-answer-to-a-future-of-new-normals/ Accessed August 2020.

Green, B. (2020). *The smart enough city*. MIT Press.
Guzman, N., Wies, M., Kozine, I., & Lundteigen, M. A. (2019). *Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis*. 2019 https://doi.org/10.1002/sys.21509. https://onlinelibrary.wiley.com/doi/full/10.1002/sys.21509 Accessed 10 August 2020.

Halegoua, G. (2020). *Smart cities. The MIT press essential knowledge series*. MIT Press.
Hines, A., & Sun, P. (2020). *Zoom fatigue: How to make video calls less tiring*. The Conversation UK https://theconversation.com/zoom-fatigue-how-to-make-video-calls-less-tiring-137861 Accessed 10 August 2020.

Karaboytcheva M. EPRS. (2020). Effects of 5G wireless communication on human health. The fifth generation of telecommunications technologies, 5G, is fundamental to achieving a European gigabit society by 2025.

Kleinhaus, J.P. (2019). *5G vs. National Security Policy Brief*. https://www.stiftung-nv.de/en/node/2511 Accessed 10 August.

Koenig, A. C., & Riener, R. (2016). The human in the loop. In D. Reinkensmeyer & V.Dietz (Eds.), *Neurorehabilitation technology*. Cham: Springer. https://doi.org/10.1007/978-3-319-28603-7_9.

Latvakoski, J., & Heikkinen, J. (2019). A trustworthy communication hub for cyber-physical systems. *Future Internet, 11*(10), 211. https://doi.org/10.3390/fi11100211. Accessed 10 August 2020.

Melanitis, Y. (2019). *Random Rhetoric, Ars Electronica*. http://www.melanitis.com Accessed 10 August 2020.

Nold, C., & van Kranenburg, R. (2011). *Situated Technologies Pamphlets 8: The Internet of People for a Post-Oil World*, Spring 2011. http://www.situatedtechnologies.net Accessed 10 August 2020.

OECD Centre for Entrepreneurship, SMEs, Regions and Cities. (2019). *1st OECDRoundtable on OECD Roundtable on Smart Cities and Inclusive Growth* https://www.oecd.org/cfe/regionaldevelopment/SmartCities-RT-Agenda.pdf Accesses 10 August 2020.

Onlife initiative. (2013). *An EC funded Report on responsible social innovation*. https://ec.europa.eu/digital-single-market/en/news/onlife-initiative-concept-reengineering-rethinking-societal-concerns-digital-transition Or why philosophy matters to policy! Nicole Dewandre Advisor on societal issues DG CONNECT European Commission https://slideplayer.com/slide/744275/ Accessed 10 August 2020.

Pauwels, E. (2019). *The New Geopolitics of Converging Risks: The UN and Prevention in the Era of AI*", United Nations University Centre for Policy Research https://www.rri-tools.eu/-/the-new-geopolitics-of-converging-risks-the-un-and-prevention-in-the-era-of-ai Accessed 10 August 2020.

RIQ News Desk. (2020). 5G on Wearables Set to Disrupt Mobility. Blog.https://www.readitquik.com/articles/immersive-technology/5g-on-wearables-set-to-disrupt-mobility/Accessed August 10 2020.

Samsung Corporate. (2020). *The Vision of 6G. Bring the next hyper-connected experience to every corner of life*., research.samsung.com https://cdn.codeground.org/nsr/downloads/researchareas/6G%20Vision.pdf Accessed 10 August.

San Juan C., Subiza-Pérez M., Vozmediano L. (2017) Restoration and the City: The role of public urban squares. Frontiers in Psychology, Vol 8, p. 2093.

https://www.frontiersin.org/article/10. 3389/fpsyg.2017.02093 Accessed 10 August 2020.
Searls, D. (2012). *The intention economy: When customers take charge*. Harvard Business Review Press.

Simmel, G. (1984). Métropoles et mentalité. In S. Grafmeyer & I. Joseph (Eds.), *L'école de Chicago* (pp. 61–77). París: Aubier.

Taoa, F., Qinglin, Q., Wang, L. W., & Nee, A. (2019). Digital twins and cyber physical systems toward smart manufacturing and industry 4.0: Correlation and comparison. *Engineering, 5*(4), 653–661. https://www.sciencedirect.com/science/article/pii/S209580991830612X?via% 3Dihub

ThingsCon. (2019). 12 & 13 December Rotterdam, the Netherlands. NGI. Forward Workshop. Read more: Data makes the world go round; Proposal for research into three policy instruments designed to strengthen (digital) autonomy https://www.nldigitalgovernment.nl/document/appropriate-use-of-data-in-public-space/ Accessed 10 August 2020.

Thwaites, K., Helleur, E., & Simkins, I. M. (2005). Restorative urban open space: Exploring the spatial configuration of human emotional fulfilment in urban open space. *Landscape Research, 30*(4), 525–547. ISSN 0142-6397.

Townsend, A. (2013). *Smart cities: Big data, civic hackers, and the quest for a new utopia*. W. W. Norton & Company.

W3C Credentials Community Group. (2020). Community Groups are proposed and run by the community. Although W3C hosts these conversations, the groups do not necessarily represent the views of the W3C Membership or staff. https://www.w3.org/community/credentials/ Accessed 10 August 2020.

W3C SSI. (2019). *A Non-Technical Discussion on Decentralized Identifier (DIDs) & Self-Sovereign Identity (SSI)* https://www.w3.org/2019/09/18-didtalk-minutes.html For a definition of DIDs, see: https://www.w3.org/TR/did-core/. For a short comprehensible presentation of the concept of Decentralized Identifiers, see in particular: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201912/Documents/KIM%20Hamilton.pdf Accessed 10 August 2020.

Wang, F., & De Filippi, P. (2020). *Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion*, Available at https://www.frontiersin.org/articles/10.3389/fbloc.2019.00028/full Accessed 10 August 2020.

Weiser, M. (1991). *The computer for the 21Ith Century*. Scientific American Ubicomp Paper after Sci Am editing https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf Accessed 10 August 2020.

Weller, C. (2018). Silicon Valley parents are raising their kids tech-free — and it should be a red flag. *Business Insider* https://www.businessinsider.fr/us/silicon-valley-parents-raising-their- kids-tech-free-red-flag-2018-2 Accessed 10 August 2020.

Yang, Z. (2018). *Situation Awareness for Cyber-Physical System: A Case Study of Advanced Metering Infrastructure*. Computer Science 2018 IEEE International Conference on Prognostics and Health Management (ICPHM).

Zhou, J., Zhou, Y., Wang, B., & Zang, J. (2019). Human–cyber–physical systems (HCPSs) in the context of new-generation intelligent manufacturing[J]. *Engineering, 5*(4), 624–636.