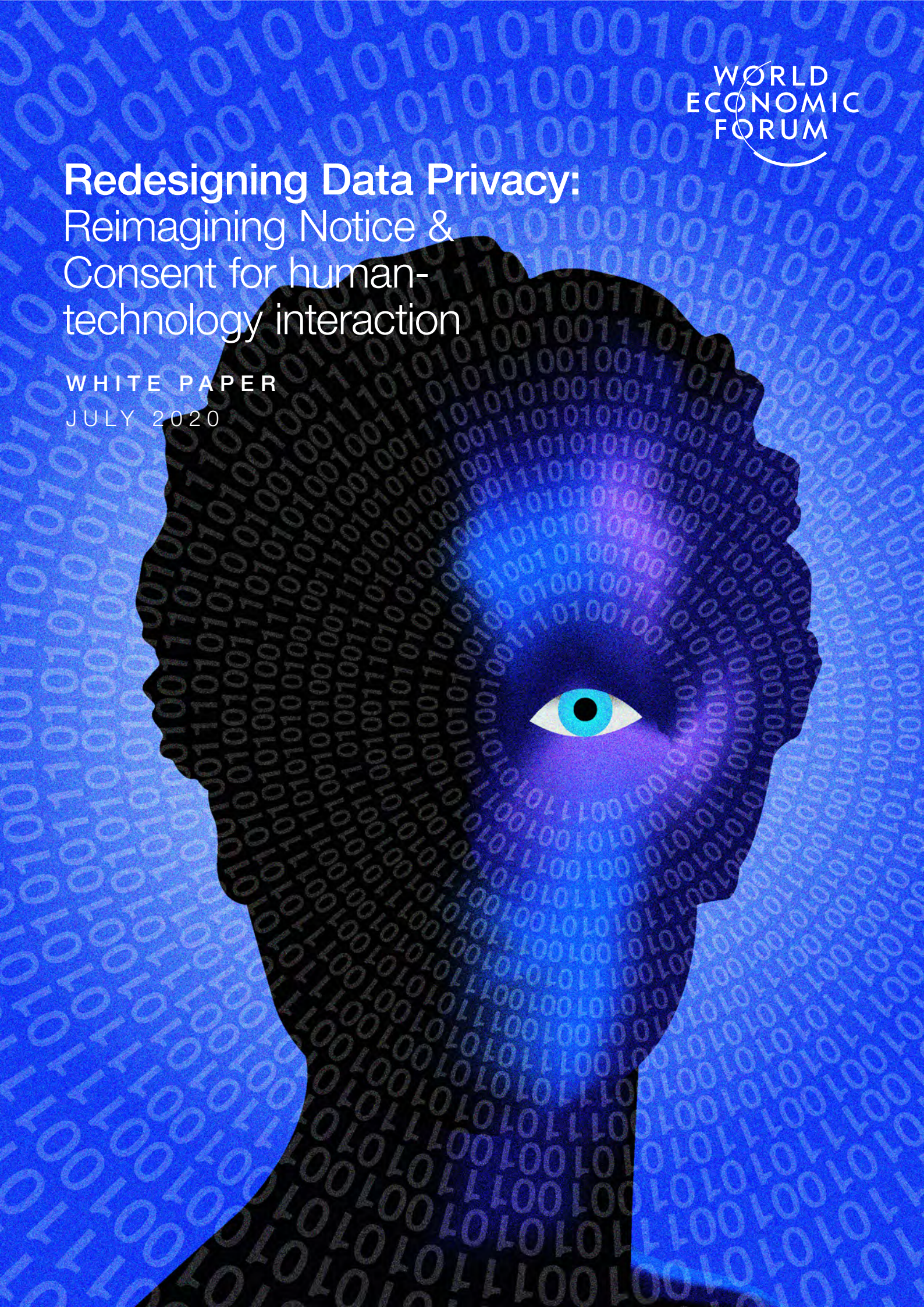
WORLD ECONOMIC FORUM

Redesigning Data Privacy: Reimagining Notice & Consent for human-technology interaction

WHITE PAPER

JULY 2020



Contents

Cover: World Economic Forum

Inside: Getty Images/Metamor Works; Unsplash/Raeng-r; Unsplash/Shane Rounce; Unsplash/Franki Chamaki

Preface

Anne Josephine Flanagan
Project Lead, Data Policy,
World Economic Forum

Jen King
Director of Consumer Privacy,
Center for Internet and
Society, Stanford Law School

Sheila Warren
Head of Blockchain, Digital
Assets and Data Policy, and
Member of the Executive
Committee, World Economic
Forum

The World Economic Forum partnered with the Center for Internet and Society at Stanford Law School and a community of policy-makers, researchers, civil society advocates, legal scholars, and industry and design practitioners to convene a set of conversations about the challenges of Notice & Consent as a norm for data collection and processing, particularly when it comes to the technologies of the Fourth Industrial Revolution. The goal was to facilitate creative thinking towards a potential redesign of the framework for all aspects of information collection, use, retention and disclosure.

Several main themes emerged from this unique assemblage of participants:

– Notice & Consent is at its core a *human-technology interaction problem*, one that necessitates an interdisciplinary group of experts from the design and technology sectors to solve it. It can no longer remain the exclusive domain of lawyers, policy-makers and engineers; rather, designers, humanitarian experts and creative technologists must have a seat at the table, as well.

– Existing approaches do not scale for either traditional digital user interfaces or the emergent world of screenless internet of things (IoT) devices, smart cities or other connected environments. Any rethinking of Notice & Consent must be scalable and anticipate these emergent contexts.

– The concept of consent, and the mechanisms for asking for it, implicate questions of ethics and normative values that the existing framework neglects. Consent that is not freely given or informed, or that is coerced, is de facto defective. A consent process must offer substantive choices to the consenting party, including the ability to withdraw consent after the fact. “Take-it-or-leave-it” models do not offer meaningful consent.

– Dynamic, unpredictable data use and reuse demands dynamic, proactive policy responses based on positive reinforcement rather than static, reactive regulation rooted in punitive approaches. In general, incentives are viewed as more powerful than prohibitions. Positive regulation that affects incentives is therefore a potential means for effecting change in this space.

– While there is a substantial body of research that offers specific design advice to improve existing mechanisms, a fundamental change in the framework is needed towards mechanisms that both scale and incorporate ethical standards.

This white paper represents a distillation of the collective efforts of the participant experts who attended workshops in San Francisco as well as that of a multistakeholder project community from industry, academia and civil society. While the approach examines the United States as a proxy for the purposes of illustration, Notice & Consent as a norm is critically assessed more generally from a design-focused perspective, and guidance is offered to both the policy-making community and technology providers in terms of updating the existing reliance on a Notice & Consent framework to address human needs and values.

By offering alternatives that place people at the centre of the paradigm, we hope that a more inclusive policy-making community can emerge to address today’s and the future’s most pressing challenges in regards to personal data collection and processing. In doing so, the empowerment of people and the opportunities for innovation should rest on more solid foundations.

Executive summary

With every year that passes, our lives are becoming more and more dependent on digital services. More than 53.6% of the world's population is online, while 93% of the world lives within reach of a 3G or better mobile network.[1] From accessing vital services such as a doctor, to ordering food online or simply surfing the web, our use of and increasing reliance on digital services continues to grow at an exponential rate.

At the same time, the way in which we interact with technology is continuously evolving: For example, some screen-based interactions are transitioning to voice-based interfaces; always-on sensors are increasingly embedded within our environments. But regardless of whether the interface is tangible or not, we are often asked to consent to the collection and use of data generated by us and about us. But how many of us truly understand what this really means? And when we are asked, does the collection and use occur in a way that fundamentally protects our best interests? Further, once we grant the requested access, is there any way to change our minds? And can consent truly be given if there is no real choice, an inability to revoke consent or lack of an informed decision because of the complexity of information provided to help make the decision more informed?

When an option to consent is given to us, there is a sense that we are empowered to make a decision, a sense that we are in control of what data can be processed, who it can be processed by, where it can be processed and for which purposes. Consent has become illusory and, through its current design and deployment, does not always operate in expected, or at times even logical, ways. As we increasingly conduct our lives online, we continue to part with more personal information, click through more boxes and increasingly seek to limit any barriers between ourselves and the service or product we intend to access.

When the permissions people grant to companies and organizations at one point in time become the gateway for everything that happens to that data in the future, that moment becomes extremely important, perhaps far beyond what could be envisaged.

The default means of setting the rules of the game on how data about someone can be used is often reliant on what is termed "Notice & Consent". Within the context of data protection and privacy, or more broadly information or onlinew data privacy, Notice & Consent functions as a primary means by which the public is provided with *Notice* about what information an organization intends to collect from a person and how they intend to use it. *Consent* is the process by which a person acknowledges and agrees to the terms of the data collection relationship.

As this paper will explore in detail, there are various concerns about how this process functions presently. These include doubts as to whether the current process is effective in educating people about the collection and use of their personal data, whether it provides them with meaningful choice and whether existing mechanisms meet the needs of the public.

The enactment of the European Union General Data Protection Regulation (GDPR) and in the United States the California Consumer Privacy Act (CCPA) increases the urgency of the need to address the flaws in current data protection and privacy norms. In the US specifically, which relies heavily on Notice & Consent frameworks, there is a possibility that federal-level privacy legislation will be passed in the nearer term. That this might occur without a long overdue reckoning with Notice & Consent mechanisms would be a missed opportunity.

Globally, countries are looking to both the GDPR and the CCPA as they consider their own data protection measures, raising the stakes with regards to how we choose to address Notice & Consent in these new regulatory environments. New laws or policies that leave existing mechanisms untouched threaten to perpetuate them indefinitely.

In this paper we examine the topic from two complementary perspectives: If we accept that Notice & Consent is not fit for purpose, how can it be improved? And what does an alternative regime beyond the terms and conditions box look like?

Part A: The challenges of consenting to data collection and processing for human-technology interaction

Introduction

More and more jurisdictions are adopting data protection and privacy rules by way of legislation. Such rules are designed to offer a level of control to individuals in respect of the collection and processing of data about them by digital services, governments or even peers, depending on the jurisdiction and the law. Despite differences in regimes, we see common themes emerging in approach. Central to most laws in respect of data protection and privacy is the tenet of legal basis, or lawful ground for collecting and processing personal data or personally identifiable information about someone. In other words, the majority of these laws set conditions for what constitutes lawful collection and processing of data about an individual.

One of the oldest and most straightforward ways for an entity to ensure that it has permission to legally handle personal data about someone is to simply seek the permission of that person. While this sounds laudable in theory, there must be some doubt as to whether, as the amount of data collected by us as individuals has vastly increased and the complexities of processing that data have risen dramatically, this method still adequately protects individuals.

While many agree on the merit of the underlying principles upon which many data protection and privacy policies across the globe are based, there is broad agreement among researchers, policy-makers, the public and industry that the current requirements of Notice & Consent for personal data collection and processing have become practically impossible for humans to reasonably accomplish without considerable simplification.

Such mechanisms usually involve the displaying of a privacy policy notice on a screen – a process most people are familiar with. Usually an individual is asked to consent to data collection at processing by ticking a box. At scale, however, even simplification falters.

Furthermore, as human-technology interactions go beyond the screen, so, too, does their ambiguity. How should an individual consent to ambient data collection by IoT devices, for example, that ambiently collect personal data via sensors and without a screen? How should people understand data processing by artificially intelligent algorithms?

In this white paper we explore in detail how we got here, where we are going and how we might better encourage both consumers and businesses to improve privacy norms for the collection and processing of personal data.

The problem with Notice

The problems with the mechanisms of Notice & Consent are both widespread and well-documented. When presented with click-through consent, privacy policies or terms of use statements, most people reflexively select "I agree". An extensive body of academic research specifically on privacy and data collection notices demonstrates that members of the public don't read them[3] and might not understand them if they did[4] and that many misinterpret their purpose,[5] assuming that the existence of a privacy policy displayed by way of notice means that the entity collecting the data offers a level of data protection when, in fact, privacy notices do not guarantee privacy. Since the terms offered are typically "take it or leave it", to decline often results in being denied the product or service one seeks, creating a disincentive for consumers to do anything other than accept the terms.

Length of notices
First and fundamentally, privacy policies, terms of service documents and similar types of online notices are nearly universally unreadable due to their length, and the public does not take time to read them.

Accessibility of notices
Because the notices and polices themselves are primarily written by lawyers, for lawyers, they are inscrutable or even incomprehensible to most members of the public. Research by information systems scholar Ewa Luger and colleagues demonstrated that the reading level in a series of terms and conditions documents was "far beyond what a functionally literate adult could be expected to understand" in the UK, raising critical questions about accessibility as well as personal agency,[6] especially given that many privacy policies and similar notices contain legal jargon or obfuscating language that makes it difficult to understand precisely what practices companies follow.[7] In 2019, *The New York Times* produced a study on privacy policies, finding similarly that the privacy policies of major consumer technology companies were written at a level far beyond the skills of the majority of the US public.[8]

In short, time commitments and readability issues alone present substantial challenges to the public in making informed decisions about the products and services, both private and public, that request their personal information.

Frequency of the notices and scalability of the process, i.e. consent fatigue
One core challenge is that the model for consent on which the notice is based simply does not scale to match the frequency and ubiquity of notices – that is, even if we make notices shorter, more readable and therefore more accessible to broader audiences, we still do not solve the issue of too many instances in which individuals are asked to make decisions about their personal information, decisions that are often binding, lasting and, depending on the jurisdiction, sometimes irrevocable. Professor m. c. schraefel and colleagues argue for systems (ubiquitous or otherwise) to adopt a concept they call "apparency": first, make it *apparent* (signal) what a system or a device is actually doing (e.g. collecting data); then, make it both *descriptively transparent* how the system functions (e.g. through written policies) and *pragmatically transparent* through proof (e.g. audits).[9]

Presentation and timing of the notices
Another related issue is the timing of consent-related decisions. Individuals are asked, typically in "take-it-or-leave-it" terms, to make decisions about their personal data at points (often when first signing up for a service) where they may not have the luxury to engage fully in the process that the current notice framework demands.

Research also demonstrates that the timing[10] of when an individual is shown a notice, as well as its visual design and framing language,[11] can affect their privacy-related decisions.

For example, the more familiar a user[12] becomes with a service, the more they are inclined to get a feel for the implications of their interaction with that technology in ways that were not apparent when they first signed up for the service. Furthermore, as software updates are pushed out, it may be necessary to reconsent to terms and conditions of that service. This is why understanding what the notice says under the current model is so important and what has led to consumer distrust of some businesses that collect and use data in a less obvious manner than could ordinarily be expected by the user.

The importance of Consent

In many cases, the privacy notices we encounter online in our day-to-day activities are routine and non-exceptional experiences, even if the stakes may vary.

We distinguish these experiences from exceptional consent experiences that require informed consent such as medical procedures, research participation, significant legal transactions, etc.: in short, circumstances with high stakes for the participant, which may or may not take place online. In some countries there are laws or specific circumstances that require or trigger a higher standard of consent than most people encounter in the course of daily events. Depending on the context and the type of information collected, it is possible there may be overlap between these areas, especially as there are calls to reconsider how notice is provided and consent obtained.

To define what "consent" means in respect of a person consenting to handing over data about themselves, their behaviour or even what type of technical device they are using, we look to the scholarship of law professor Nancy Kim, whose book *Consentability: Consent and Its Limits*[13] presents a thorough overview of the topic. According to Kim, consent is "typically a conclusion based on the presence or absence of three conditions: an intentional manifestation of consent, knowledge, and volition/voluntariness".[14] Consent must be expressed to the other party through words or actions, and that communication must be intentional, meaning that the "reason or purpose for the manifestation of consent is to communicate consent to the act" in question.[15] The consenting party must understand what they are consenting to; "knowledge requires both *understanding* and *information* in light of the consenting party's *motive* for consenting".[16] Finally, consent must also be voluntary, "intended rather than reflexive", and defined by an "absence of undue pressure or coercion".[17] In the context of this white paper, an individual providing consent for data collection would ideally, prior to consenting, understand the collection practices to which they were consenting; do so freely without being coerced or manipulated; and be provided with a means by which they could communicate their consent clearly and affirmatively.

In the US, consent as it pertains to data collection emerged from contract law, which according to Kim "does not require actual (subjective) knowledge". Instead, contract law substitutes *capacity* and *access to information*, or *Notice*, for knowledge.[18] In the majority of instances when individuals are asked to provide their consent online, the consent process itself is a first step in contract formation, or entering into a contract, with a website or service provider.[19] In US law, knowledge requirements are dependent upon the threat to one's autonomy. For example, a medical procedure that poses "a high-level threat" to one's autonomy will be regulated more thoroughly than a form asking for emails to be used in a marketing campaign. However, in most online contexts there is no legal obligation for organizations to provide a notice that can be fully read and understood by any individual, or to obtain affirmative, voluntary consent. Instead, a company's privacy policy, which describes data collection, is typically a legally focused document not constructed for the end user's easy and rapid consumption. There has been a recognition by some companies that privacy policies are difficult to navigate and some companies have stepped forward with improved interactive notices and so-called privacy check-ins.

How did we get here? A history of Notice & Consent

Notice and Consent are key components of the Fair Information Practices (FIPs), a set of principles developed in the late 20th century in response to the growing digitization of information.

The original FIPs, as drafted by the highly influential HEW Report in 1973, do not contain Notice & Consent. The Organisation for Economic Co-operation and Development (OECD) modelled its FIPs on these in 1980 and added consent, but also kept the original focus on the principles of purpose limitation, transparency in the sense of giving individuals access to their data, correction of data and accountability of the organizations that collect and use data. While there have been several versions of the FIPs over the years, they tend to restate the same core set of principles, with a focus on individual control over information and "procedural safeguards for data handling rather than substantive bans on practices".

Fair Information Practice Principles

According to the the Fair Information Practice Principles, as adopted by the US Federal Trade Commission in 1998 the following common terms are defined:

Notice: Data collectors must disclose their information practices before collecting personal information from consumers

Choice: Consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided

Access: Consumers should be able to view and contest the accuracy and completeness of data collected about them

Security: Data collectors must take reasonable steps to ensure that information collected from consumers is accurate and secure from unauthorized use

In 2020, the US remains without comprehensive data protection legislation at a federal level.

In the US, which lacks a federal-level data protection or privacy law covering all personally identifiable information,[22] the FIPs have become a primary means of governing how data is collected in the online sphere. Bob Gellman notes that "[n]otice and choice is sometimes presented as an implementation of FIPs, but it clearly falls well short of FIPs standards".[23] According to Chris Hoofnagle, while the FIPs were recommended by the Federal Trade Commission as a basis for omnibus federal-level US privacy legislation in the early 2000s, the idea stalled, and in 2020, the US remains without comprehensive data protection legislation at a federal level.[24] Within the US, state-level laws have driven changes on Notice requirements, as has the federal-level Children's Online Privacy Protection Act (COPPA) law designed to protect the personal information of children. While FIPs are unenforceable in the US, contract law is on a solid legal footing. Upon entering into a Notice & Consent-style framework in the US when that relationship is business-to-consumer, the consumer effectively signs a contract. The normalization of this process has been necessary for business to ensure legal certainty in the obtaining and processing of personal data, particularly with the explosion in free online digital services.

The evolution of data protection in Europe followed a different trajectory. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108), adopted in 1981, remains the primary source of data protection law for Council of Europe member states. Later on, these provisions were further developed, in a narrower European Union (EU) context, in the Data Protection Directive 95/46/EC,[25] which as of 2018 was replaced by the EU General Data Protection Regulation 2016/679. Foundational to the development of EU law in this space were separate rights of data protection and privacy leading to laws governing the protection of the collection and processing of personal data, and the privacy of personal data in transmission, including in respect of cookies. These are reflected in the GDPR and the ePrivacy Directive respectively. Consent plays a greater role in the confidentiality of telecommunications framework (under the right to respect for private life and the ePrivacy Directive)[26] than it does under the data protection framework (under the right to the protection of personal data and the GDPR). Under the GDPR, consent is just one of six legal grounds for data collection and processing under EU law, while Notice (in the sense of providing information to individuals about what will happen with their personal data) is required for processing under all lawful grounds, including for processing based on legal obligations of the organization collecting or using the data. The addition of five other legal grounds for the collection and processing of personal data under the GDPR de-emphasizes a reliance on Notice & Consent and attempts to recognize its limitations as a one-size-fits-all method,[27] which is very much in contrast to the FIPs process.

Outside of the EU and the US, Notice & Consent has become a consistent international norm given its extraterritorial reach in respect of certain conditions and trade incentives for non-EU economies to align with the EU approach.

Despite two decidedly different trajectories, Notice & Consent has clearly become part of both the EU and US data protection and privacy landscapes. Outside of the EU and the US, Notice & Consent has become a consistent international norm in varying degrees, due in part to the overwhelming reach and trade incentives built within the GDPR that push non-EU economies to align with the EU approach.

The enactment of the GDPR and the CCPA also increases the urgency of the need to address the flaws with Notice & Consent as a norm. In the US specifically, they provoke the possibility of passing federal-level privacy legislation in the nearer term. If this were to occur without a critique of Notice & Consent mechanisms, it would be a missed opportunity as countries look to regulation within the US and EU as models to consider as they implement their own data protection measures. New laws or policies that leave existing mechanisms untouched threaten to perpetuate them indefinitely. Regulatory certainty remains essential and it is business that is now pushing for the US to have a more EU-like approach to alternative models for data collection and processing such as legitimate interest.

Notice & Consent: an assessment

Privacy scholar Daniel Solove notes that "[c]onsent legitimizes nearly any form of collection, use or disclosure of personal data … individuals cannot adequately self-manage their privacy, and Consent is not meaningful in many contexts involving privacy".[28]

A 2014 Obama-era report from the President's Council of Advisors on Science and Technology (PCAST) described Notice & Consent as follows: "[N]otice and Consent fundamentally places the burden of privacy protection on the individual – exactly the opposite of what is usually meant by a 'right'. Worse yet, if it is hidden in such a Notice that the provider has the right to share personal data, the user normally does not get any Notice from the next company, much less the opportunity to consent, even though use of the data may be different."[29]

According to Woodrow Hartzog, "Notice is quite attractive to regulators. Lawmakers like mandated Notices as regulatory instruments because it costs companies very little and preserves a fair bit of freedom for companies to experiment and design as they wish in the name of innovation … for designers, terms of use can be like the elephant in the room: designers can construct an environment that acknowledges the impact of the terms, or they can ignore them, oblivious to any contradictions that might arise between the messages conveyed by design and by contract."[30] Crucially, Hartzog argues: "When privacy law ignores design, it allows Notice to become rote and ineffectual. Design can be used to obscure Notice and exploit our limited ability to understand what is being conveyed."[31]

It is the understanding of those "realistic assumptions about human intent and behaviours" and how to accommodate them that the design community brings to the Consent debate.

In many, if not most, online contexts today, consent is offered as a "take-it-or-leave-it" option, with a rejection of consent typically presented as "leave-it".[32] Kim argues that "the consenting party must have access to the information in a form and at a time which helps that party *understand* material and relevant information and the consequences of consent. The presentation of the information must take into account the realities of how humans make decisions in given contexts, instead of presupposing a rational actor making decisions under ideal circumstances (unlimited time, sufficient resources, technical or specialized knowledge of the subject matter, detached emotional state)."[33]

"I accept" buttons are not inevitable. In their book *Re-engineering Humanity*, Frischmann and Selinger say, "Contract law could have accommodated changes in economic, social and technological systems differently. What we have now is neither necessary nor inevitable. Fortunately, contract law can still change."[34] If contract law can change, then Notice & Consent can move beyond its current contract law norm in the US.

According to Kim, "When the stakes are high and pose a grave threat to autonomy, whether individual or collective, the conditions of consent must be at their most robust. If they are not, then the rhetoric of consent should not be used to provide either the legal or moral justification for the consent-seeker's actions."[35] The aforementioned PCAST report asserts that this results in a "non-level playing field in the implicit privacy negotiation between provider and user. The provider offers a complex take-it-or-leave-it set of terms, backed by a lot of legal firepower, while the user, in practice, allocates only a few seconds of mental effort to evaluating the offer, since acceptance is needed to complete the transaction that was the user's purpose, and since the terms are typically difficult to comprehend quickly."[36]

It is clear that Notice & Consent as a norm places an undue burden on the person.

What's at stake without reform

When we rely only on Notice & Consent, we neglect to develop proper policies for the collection and treatment of personal data across the entire digital value chain, including:

1. **We fail to properly account for the reality of screenless technologies**

While the laws with which we are familiar – for example, GDPR, CCPA, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, Brazil's General Data Protection Act (LGPD), the Protection of Personal Information Act (POPI) in South Africa and the Act on Protection of Personal Information (APPI) in Japan – are in effect built for a world of screens, the reality is that data is also being collected ambiently through touch sensors, IoT devices, cameras and other ambient computing devices. The GDPR, although it has other legal grounds for data collection available, applies consent requirements to consumer IoT devices – which makes them difficult to use legally within the EU. The CCPA, in contrast, largely requires notices and opt-out choices rather than consent, and affirmative consent is not required under CCPA except from minors if companies want to sell their personal information.

This reliance on Notice & Consent for screenless technologies is inappropriate given the ubiquity of data collection when interacting with such technologies.

2. **We fail to provide adequate certainty to companies that could encourage them to find innovative solutions to protecting our privacy**

The GDPR is technically technology-neutral.[37] However, with many organizations relying upon external law firms and in-house counsel to implement GDPR-compliant notices, its implementation can often fall down at a user experience (UX) perspective, with the result that UX designers then implement "nudges" after the event in the form of UX adjustments. Some digital service providers have sought to close this gap by encouraging a parallel design process, but without clear guidelines from regulators the task remains challenging and the incentive to move away from screen-based notice regimes is minimal.

The result is that we fail not only the people and their rights, expectations, well-being and opportunities in this new digital world but also the innovators and companies who are advised to rely on Notice & Consent more often than is necessarily appropriate as it represents a safe legal ground when no better alternative is clear.

3. **We fail to account for the reality of secondary data use**

The emphasis on setting the rules at the point of collection of the data fails to take account of the reality of the value of business-to-business (B2B) sharing of personal data, data analytics, future transactions and especially future unforeseen use cases of the data – uses with which a person may be in agreement, but cannot consent to because it is too late. Once the data enters the value chain, seeking reconsent is extremely challenging when it comes to repurposing the data.

In order to accommodate the challenges of future computing technologies we are presented therefore with two options.

a. Notice & Consent mechanisms must be fundamentally rearchitected in order to account for human needs. At their best, they would embody a social engagement that is designed to visualize and support people's ongoing relationships with their data, including the ability to renegotiate or withdraw consent, rather than a discrete one-time taking by a data processor, and would by design inform and promote comprehension, rather than merely signpost, allowing individuals to make fine-grained choices about their data.

b. Notice & Consent mechanisms must be fundamentally replaced: nowhere is this issue more urgently illustrated than as we consider the use of new forms of digital technologies without traditional screens, such as voice-based interfaces and internet of things (IoT)-based devices and applications. If the current system is barely fit for purpose under existing screen-based constraints, it is utterly ill-equipped to manage a world in which data collection happens through IoT devices inside the home as well as in public spaces.

Regardless of which option we take, the importance of people, their rights, their experiences and how they can navigate the always-on ubicomp world of the Fourth Industrial Revolution, solutions must be designed with people in mind.

Part B: The opportunity of an alternative approach: why we need human-centred design

Redesigning Notice & Consent: a human-centred design approach

Existing Notice & Consent mechanisms disregard the complex reality of human psychology.

We have already explored how despite thirty years of dynamic evolution of the internet and the more recent dawning of the Fourth Industrial Revolution, Notice & Consent in the digital realm remains locked into predominantly skeuomorphic virtual representations of paper contracts.

Existing Notice & Consent mechanisms are based on the classic model of the rational individual who can read and understand a privacy policy, calculate the trade-offs of the benefit of the service versus the information collected, and make an informed choice. This process disregards the complex reality of human psychology, specifically individual decision-making processes. Studies in the fields of human-computer interaction, behavioural economics and social psychology have demonstrated that people's choices are influenced by a multitude of factors that cloud rationality: Affect, cognitive heuristics, social desirability, economic need and interface design, among others, all play a role in shaping an individual's decision to consent or not to the use of their data.

Questions raised on this topic by the project community included: How can we account for these "irrational" factors to improve the state of Notice & Consent mechanisms? How do we unburden consumers from the cognitive load of having to understand the long-term implications of the decisions they make today? Further, most consumers are unaware of the many forms of data collection conducted by third parties on websites and within mobile apps. How do we create, in other words, a system of Notice & Consent that adheres to "protection without comprehension"?

One way to reconceptualize the human practices that privacy should protect is by way of changing how we think about the people who constitute the users. Current Notice & Consent approaches begin from a view of the user as primarily a consumer – as a rational agent motivated by economic interests whose risk calculation in sharing information rests on a calculus of economic harm. This approach misses the mark in terms of capturing the diversity of human activity that takes place today on the internet. We don't merely purchase goods or services; many of us live a social life online, connect to our communities or access public services. The digital footprints that we leave across the internet on a daily basis affect us as humans, not merely as consumers.

In contrast, existing mechanisms of Notice & Consent correspond largely to a world of e-commerce. They do not map to the fact that our actual lives – our social identities –are in many ways defined by the dynamics of our online behaviour, both explicitly and implicitly. Our challenge in reconstructing mechanisms of Notice & Consent is to consider privacy not only in terms of consumer protection but also as a human right. Because privacy and information-sharing online now affect so many facets of our lives – the way we vote; the way we relate to friends and family; the quality of our mental and even physical health – we need a broader understanding of privacy than simply the consumer context, and it needs to be used to reconceptualize consent mechanisms that serve those privacy values.

People absolutely need help with managing their data in complex environments, and privacy frameworks and tools should support these needs. The aim should be a system that can guide and inform consumers about the implications of their choices, whether through human advice-giving, data visualizations or digital tools to aid in managing our data relationships, including to whom we have provided consent, and how to revoke it.

A key challenge is to find a compromise between the extremes of a) providing broad consent and ceding all control of one's privacy, and b) requiring "microconsent"[38] every time one's data is used, resulting in an inability to fully understand every consent request and consent fatigue. Solutions should both maximize access to the data and protect each individual's right to control of privacy and data use transparency. Solutions should not require permanence; the right to revoke consent/ access should ideally be preserved for all individuals.

What is human-centred design?

US professor and researcher Don Norman is credited with helping to define the concept of human- (or user- or people-) centred design (HCD). As he wrote in *The Design of Everyday Things*, "user-centered design [is] a philosophy based on the needs and interests of the user, with an emphasis on making products usable and understandable".[39] HCD is inherently interdisciplinary, interleaving psychology, cognitive science, anthropology and human-computer interaction into both a research practice and a professional specialization. The design firm IDEO is one of HCD's most famous adopters, integrating HCD into its firm's practice as well as producing design kits and field guides to HCD to promote its adoption.[40]

The core thrust of HCD is to put the needs of people at the centre of any technological system, and to assess and understand those needs by engaging directly with the people whom the technology will serve. In 2018, Norman published *Four Fundamental Principles of Human Centered Design and Application*,[41] in which he elaborated on the people-centred focus of HCD: "Much of today's systems, procedures, and devices are technology-centered, designed around the capabilities of the technology with people being asked to fill in the parts that the technology cannot do. People-centered means changing this, starting with the needs and abilities of people. It means considering all the people who are involved, taking account of the history, culture, beliefs and environment of the community. The best way to do this is to let those who live in the community provide the answers."

Academic research yields many recommendations that, if followed by businesses or adopted by regulators, would make privacy notices simpler, easier for many to understand and more transparent.[42] Why haven't these recommendations been widely adopted? One of the core issues is that companies are not incentivized to change the status quo without assurance that it does not amount to increased legal risk. For this reason alone, it is necessary to heed the importance of the recognition of alternative methods by policy-makers for establishing the legality of data collection from people when they interact with technology. It is difficult for companies to make these changes due to the traditional barriers of time and cost resources, but the status quo is systemic.

One of the most glaring systemic issues is the fact that many companies may be detrimentally affected by improving notices and increasing transparency. The majority of entities that collect personal data benefit from the status quo and understand that increasing transparency about historically opaque data collection practices can affect business, notwithstanding that there are many non-business cases in which the sharing of personal data via Notice & Consent may be used, such as in COVID-19 contact tracing apps. Requiring individuals to opt in rather than opt out[43] of data collection also discourages data sharing. Without additional incentives or regulation, companies will not willingly adopt these changes[44] due to a combination of: (1) a desire for the status quo to prevail; (2) not enough pressure on companies to make any changes; (3) technical compliance paying lip service to the law; and (4) user apathy. This is now changing, and people are more interested in how their personal information is being processed. Organizations are becoming more transparent in terms of data collection, and regulation has helped, although regulation alone is not going to solve the problem completely. For example, the current compliance mechanism for cookies in the EU demands separate consent, opt-in options, different boxes for different purposes etc., and although many companies implement and comply technically, the individual ultimately gets to decide how much they care to interact with the banner notifications compared to how much they just want to use the services. For this reason, many companies have gone beyond legal requirements and notices in terms of educating their users, and in doing so can build increased trust with their users.

There are also ethical questions regarding whether data created in one context (e.g. healthcare data) should be made available for use in another context (e.g. consumer goods), even if the notice communicates this use. Article 6 of the GDPR addresses this issue by stipulating five alternative legal grounds[45] for data collection depending on appropriateness, with an expectation that relying upon Notice & Consent alone as a rationale for justifying data collection practices is insufficient in all circumstances. It also provides overarching data processing principles, including the concept of "purpose limitation", which ensures that further legal permission is required for any further processing of personal data, something that is amiss in the US's "take-it-or-leave-it" norm of Notice & Choice.

This approach acknowledges the inherent limitations of Notice & Consent: Because it can be complex, manipulative and incomprehensible to many, relying upon it alone as a rationale for any kind of data practice does not guarantee that those who give their consent truly understand what it is they are consenting to and may be wholly inappropriate.

According to Nancy Kim, "[t]he presumption of consent which arises from an action, such as signing a document or clicking on an 'accept' icon, is entwined with the 'duty to read.' Rather than being an affirmative obligation, the duty to read is a presumption that someone who has signed a document (or clicked to accept online terms) has read the terms that the document contains."[46] But we are not simply dealing with the legal rights and responsibilities of the respective parties entering into an agreement for the provision and receipt of goods and services. Notice & Consent is very much a mechanism where an organization uses an individual's personal information unrelated to the provision of such services. A design-centred approach to Notice & Consent raises questions about the limitations of a model that relies upon a duty to read (and understand) the contexts in which it may not be appropriate, and the underlying ethics of the data collection itself. Thus, it is important to raise critical questions about whom these mechanisms benefit, whom they exclude or leave behind, and the contexts in which placing the burden of reading and understanding wholly on the shoulders of the public creates more harm than benefit.

Automating Notice & Consent: an idea 20 years in the making

One of the suggestions adopted by our project community – to create a software-based agent to manage and negotiate individual privacy preferences – builds on more than 20 years of extant research. The idea of automating privacy preferences and negotiations in internet browsers originated in the late 1990s with the development of the Platform for Privacy Preferences (P3P) standard.[47] Lorrie Cranor of Carnegie Mellon University led the effort, which she described in her paper, "Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice": "Early proponents of P3P described web browsers that could read privacy policies, negotiate with websites and take actions on their users' behalf without interfering with the web browsing experience. P3P was envisioned as a tool that could facilitate a market for privacy, enabling individuals to shop around for websites that would match their privacy preferences, refusing to do business with those they found unacceptable, and perhaps accepting payments or discounts in exchange for data."[48] While P3P 1.0 was finalized in 2002, a lack of regulation as well as incentives for industry to implement P3P resulted in the abandonment of the standard.

Based on her first-hand experience with developing P3P, Cranor notes that without both regulation that sets a baseline for allowable information collection, and use practices and robust enforcement, not only would there be a lack of incentives for companies to honour a protocol-based agent, "there would also be significant incentives for companies to game the system and misrepresent their policies".[49]

In short, it is overly simplistic to look back over these efforts and conclude that an important hindering factor was that they were ahead of their time; while the growing ubiquity of smartphones might help bridge earlier gaps in implementation and connect new avenues for negotiating data collection (such as ubiquitous computing), the fundamentals remain: Without regulation, these proposals are likely to die on the vine.

Collective privacy

While we tend to understand the concept of individual privacy well, it is important to note that privacy is not necessarily limited to individual concerns and can also be collective in nature. Data that people share about themselves can also reveal things about family, friends, colleagues, neighbours etc., and it unlikely that those people will be aware of this information sharing, let alone be in a position to provide consent. Apart from privacy concerns, the consequences of providing information about people of the same race, gender and age group can create the potential for political or economic discrimination or exploitation of more than one person. Genomic data, for example, can reveal information about one's relatives and thus needs to be handled particularly carefully. Due to its highly sensitive nature, the collection and processing of genomic data is particularly controversial in this sense, and beyond relying on just Notice & Consent, there are clearer safeguards in some jurisdictions than others. For example, in the EU genomic data is classified as highly sensitive data under the GDPR and this requires a higher standard of care.

A grounded example of a project that seeks to fully understand collective privacy and consent in the context of vulnerable populations is INTUIT,[50] an interaction design project seeking mechanisms

for the "Trusted Sharing of Personal Health Data to Live Well with HIV" with a review of consent at its core. The project is a collaboration of experts in the lived experience of HIV, HIV medicine, public health, human computer interaction, design, health psychology, health informatics and applied ethics, which moves beyond the analytic, logic-oriented and individualistic approaches to consent towards more empathic and collective approaches. People living with long-term stigmatized health conditions, such as HIV, require high-level protections for their data. However, the initial findings of the project also show that individuals within this community have a strong desire to balance this against the wider needs of the community, necessitating models of community or collective privacy. One of the outcomes of the INTUIT project will be the development of a human-centred, co-produced consent model.

In both the genomics and INTUIT examples we see the importance of collective privacy for use in specific circumstances. The way in which Notice & Consent (or other legal bases for data collection and processing as relevant) is managed is nuanced by the specific contextual circumstances of the use cases and the implications for the collective privacy of a wider population than just one individual.

By placing people rather than the idea of a consumer contract at the centre of the Notice & Consent paradigm, we start to unlock human-centred design as a solution to better data privacy.

Alternative models: thinking outside the box

Central to the challenge is addressing fundamental ethical principles.

Any alternatives to the existing Notice & Consent need to be relatively globally applicable, technology-neutral (beyond the screen) and as explicitly grounded in ethics as possible. This means recognizing the needs and vulnerabilities of the least privileged while also respecting the purpose for which the data is being collected, such as minimizing reliance on text that requires high levels of literacy.[51] Technology is fast, but regulation is often slow. In another five to 10 years the internet will look very different from how it does today. By then, many of the tactics discussed today will *already* be inapplicable to huge swathes of the global internet.

In this section, we discuss several of the themes that emerged from our work on this project, including our October 2019 workshop and the ongoing collaborations with our larger project community. These themes provide the foundation upon which this community developed the specific recommendations presented later in this paper.

The working group focused largely on key values and principles rather than explicating specific design improvements or design methods. This focus speaks to the group's understanding that central to the challenge is addressing fundamental ethical principles, and not simply surface-level fixes. We must solve the human problems before we define the technical solutions. How do we reconcile our pre-digital expectations and requirements of privacy as technology's reach into people's everyday lives continue to grow, not just in the case of commercial digital services but in healthcare, utilities and the provision of government and public services?

The necessity of a global technology-neutral approach

The adoption of the GDPR was an international game changer for data protection and privacy. The GDPR's principles have extended beyond Europe to become a new de facto global standard as other countries contemplate meeting GDPR adequacy standards or consider updating or adopting data protection laws of their own. Many countries have already passed such legislation.

The GDPR includes design guidelines for Notice & Consent mechanisms that clarify the existing Notice framework (primarily by describing prohibited types of interaction design, such as pre-checked Consent boxes). The GDPR is clear that consent should not be bundled up as a condition of service unless it is necessary for that service. Article 7(4) states: "When assessing whether consent is freely given, utmost account shall be taken of whether … the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract." And Recital 43 says: "Consent is presumed not to be freely given … if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance."

The CCPA in the US contains minor requirements for improving the presentation and content of privacy policies, but does not otherwise alter the core Notice & Consent framework.

Our community strongly recommends that future changes to Notice & Consent must be, to the fullest extent possible, part of a multistakeholder global regulatory approach. A single set of design solutions will not be applicable across the globe, but it is imperative that including an international set of participants is vital to ensuring an equitable outcome. There was considerable concern in the project community about the lack of technology expertise in many governments today and, in particular, a deficit of policy-makers or staff with a human-centred design expertise. While there is no quick solution for building technological expertise in the public sector, we want to make policy-makers aware that adding expertise that includes human-centred design – not merely technologists – is vital to the success of future endeavours.

Making explicit ethical frameworks

“ Awareness and control are the two core tenets of human-computer interaction design.

A factor in common between both the GDPR and the CCPA (and other modern data protection and privacy regulations) is influence of the legacy of the FIPs, which primarily value *individual control* and *personal autonomy* as the goals of data protection. This approach has several limitations: First, as discussed earlier, the Notice & Consent mechanisms that the FIPs enable do not effectively scale to handle the complexity of the data-sharing relationships that most individuals experience. Awareness and control are the two core tenets of human-computer interaction design as described by Bellotti and Sellen[52] in 1993. Such awareness is key to autonomy, but absolute control and autonomy at an individual level appear to be impossible in a world as deeply interconnected as the one we now live in. Many individual data-sharing decisions have impacts beyond the individual, through social relationships as well as through increasingly networked publics. Centring privacy only in terms of individual choices neglects the larger impacts those choices have on our wider societies, suggesting that we need to consider other ethical values implicated through data collection and explicitly incorporate them into a new approach.

Our community identified the need to make explicit the ethical frameworks that guide regulation, and to consider a broader set of values than we have typically seen implicated in technology design. In the US, one area of focus has been to call for legislation mandating fiduciary responsibility, or duties of care, by data collectors, who could be held to a standard of doing no harm in their collection and use of individual data.[53] An ethics-based approach also brings up broader questions about finding ways to protect the privacy rights of those who have been the most negatively affected by current data collection practices – often those most socioeconomically marginalized.

We discuss the values they identified below. However, we must also acknowledge upfront that this approach will undoubtedly run into obstacles in a global community; some nations or cultures may prioritize a different set of values from those identified in this paper.

Consent and social justice

Many members of the project community carried a heightened awareness of the need to account for the needs and concerns of the most vulnerable in our societies, and to ensure that they are included in future design efforts. There was a specific call to recognize the disparate impact of data collection and use on different socioeconomic and racial groups. To a large extent, existing technologies as well as Notice & Consent mechanisms reflect the reality of a world in which marginalized people have been excluded both as participants in design processes and as beneficiaries of consumer technologies. Often marginalized people lack trust in current consent frameworks and institutions, due to historic abuses, and choose not to consent, exacerbating the disparity challenge. If we continue to develop solutions without including those perspectives, then we are in jeopardy of reinforcing and accelerating existing societal divisions between the powerful and the powerless. We are also in danger of losing the necessary contrast in the aggregate data to make the discoveries being sought. Redesigning Notice & Consent will require multistakeholder participation not only from governments, corporations and academic institutions from around the world to develop an inclusive dialogue but also from members of those communities, and their advocates, if we are to develop an inclusive policy-making dialogue.

We cannot assume that every person comes to the table with the same resources. This is especially true in the realm of technology, where those with less education or familiarity with technology may not be able to accurately calculate the cost of the trade-offs involved when attempting to balance privacy with data collection. Further, those with the least power in society are at the greatest disadvantage when negotiating with powerful actors. A human-centred approach to redesigning Consent must consider the human population as a whole, and take care to account for the needs and experiences of vulnerable populations.[54]

Building Consentful Tech: FRIES

The Consentful Tech Project[55] aims to ground digital consent in ethical practice, comparing it to the process of obtaining consent in the physical world. In its online publication, the project draws on Planned Parenthood's FRIES model[56] of consent (freely given, reversible, informed, enthusiastic and specific) as an example of a model for obtaining meaningful consent between individuals. Given that online consent today is often not freely given (in that the terms are typically non-negotiable and refusing the terms means not accessing the product or service), irreversible, not well-informed, and lacking enthusiasm, and that it often includes terms that are far broader than what might be required to immediately access and use a service, the FRIES model provides a useful contrast to, and a highlight of, some of the more grievous aspects of the current framework.

The importance of Industry in policy-making

“Industry must be included in this conversation at all stages or we risk a race towards compliance for compliance's sake.

Industry has a crucial role to play in unlocking solutions to this very real puzzle due to the fact that industry norms often precede policy-making. It is industry that designs and markets products that collect such data, sometimes for functional purposes and sometimes as part of a business model. Industry must be included in this conversation at all stages or we risk a race towards compliance for compliance's sake without meaningfully improving both privacy outcomes for people and innovative outcomes for business and wider society.

Redesigning Notice & Consent also requires contributions from the greater “design community”: the class of professionals and researchers that commonly includes UX designers, visual designers, interaction designers and information architects, all of whom typically practise “human-centred design” or “user-centred design”. Academics who conduct research in this area hail from fields such as human-computer interaction, computer science, information science, cognitive psychology and communication studies. These represent areas of expertise that policy-makers sometimes lack.

In essence, human-centred design methods put the needs and limitations of the human user at the forefront of any design activity. It is essential that reforms of, or alternatives to, Notice & Consent frameworks must be based on principles of human-centred design in order to be effective.

How do we move forward?

Notice & Consent mechanisms in digital environments – the visual appearance of notices, choice of language, format and timing of presentation – matter critically to the public as they weigh up with whom they should share personal information.

The model of Notice & Consent, therefore, is no longer relegated strictly to the legal realm; it is inherently a human-technology interaction problem, one that requires the expertise of those professionals and academics versed in human-computer interaction issues and, ideally, public policy and ethics.

As discussed above, taking a step back to adopt a global, technologically neutral approach that is ethical, includes an awareness of society and involves industry is key. And, critically, professional UX designers – who fundamentally understand how people interact with technology – will need to tap into design thinking to try to address this intractable problem.

Part C: Ideas to explore

What are the characteristics of better alternatives?

1. **Agency vs. usability**
   Not only are existing mechanisms generally not user-friendly, because they do not allow for negotiation or revocation, they also do not give consumers agency: the option and means to act in their own interests. Redesigning Notice & Consent mechanisms to make them more usable does not ensure a greater degree of agency. In fact, reducing friction in interfaces – often a goal of design – may in fact reduce one's ability to act on privacy-related choices in one's own interest. Consent mechanisms must allow for individual agency, whether that be an ability to negotiate the terms of consent or requirements to explicitly opt-in (rather than opt-out) of various forms of data collection and use, for instance.

2. **Design-focused collaborations and tools**
   We can focus on global public participation by encouraging the interaction of designers, technologists, the public sector and other stakeholders in explicitly public activities focused on problem-solving for the public sector. One example is "design jams" that bring together diverse audiences for open collaboration and problem-solving with a design focus.

3. **Real choice**
   This is a design approach that promotes the choice of revoking choice – or in other words, design of Notice & Consent that heeds the principle of temporality of consent. Consent is not permanent or eternal, but the practicality of revoking consent may be difficult to achieve for emerging technologies such as IoT and artificial intelligence (AI) that require a constant flow of data for their operation and learning, which then becomes embedded in the wider system.

A global framework is needed that takes into consideration lenses of meaningful consent – principles such as: transparency; comprehension; control; accountability and explainability; prevention of exploitation, manipulation, and discrimination. In other words, we need to move towards meaningful "choice" instead of merely "consent".

Nine ideas to explore

The project community explored different ideas aimed at reforming both the basis and the mechanisms for Notice & Consent.

We must note that these nine ideas do not present a detailed roadmap of precisely where to go next. Instead, they represent pieces of a larger puzzle: the product of creative brainstorming based on thinking beyond the current constraints of the Notice & Consent regime. They are a starting point towards opening a conversation for future creative thinking and collaboration. No idea is meant to be a singular solution or one-size-fits-all approach, and each idea has its own benefits and drawbacks that should be carefully considered. In addition, ideas can be combined with each other for optimal outcomes.

1 Data visualization tools for policy-makers

Since the effect of privacy policies and other data protection mechanisms are generally discussed in the abstract, there is a need to illustrate the actual impact of data collection and its use based on real user experiences. However, the lack of both technical and design expertise among many policy-makers and politicians raises difficulty in policy-making, notwithstanding that expert witnesses are often invited to provide viewpoints and that policy-makers generally welcome lobbying. This technical and design knowledge deficit can, however, negatively affect regulation, particularly the ability to

anticipate the evolution of technology and therefore the appropriate policy response at government level.

The goal of data visualization is to provide policy-makers with tools to create prototypes, graphics and visual examples in order to demonstrate how regulatory outcomes affect individuals directly, helping policy-makers to understand the user experiences implicated by their proposed regulations and rules. Data visualizations could highlight marginalized or excluded experiences in the policy-making process, particularly if multiple partners assist as a coalition in the creation of visualizations.

One proposed outcome is to support the intersection between design and policy by creating an organization to support this work, which includes UX designers and other relevant experts beyond lawyers. Given the convening power of the World Economic Forum, the expertise of the project community and the Forum's position as a platform for public-private partnership, the establishment of an advisory committee of sorts could be helpful to policy-makers in navigating future personal data laws, including those based on the premise of Notice & Consent that seek more fit-for-purpose and granular case-based outcomes.

2 Harm assessment process

In consenting to a Notice requesting their personal data, consumers in the US are signing a contract that protects the company's interests if it does not violate the terms. In contrast, in the EU, an entity planning to collect and process data must choose an appropriate lawful basis, a choice that will be borne before the respective data protection authority in the case of a complaint. Legitimate interest is one such lawful basis for data collection and processing that is available under GDPR Article 6 (1) f, which states that processing is lawful if it is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".[57]

As per Working Party 29, "consent as a legal ground has been analysed in Opinion 15/2011 of the Working Party on the definition of consent. The main findings of the Opinion are that consent is one of several legal grounds to process personal data, rather than the main ground. It has an important role, but this does not exclude the possibility, depending on the context, that other legal grounds may be more appropriate either from the controller's or from the data subject's perspective. If it is correctly used, consent is a tool giving the data subject control over the processing of his data. If incorrectly used, the data subject's control becomes illusory and constitutes an inappropriate basis for processing."

The idea that companies should be conducting impact assessments vis-à-vis consumer harm is not new. This type of procedure, which backs up alternative legal bases for data processing, has not been adopted in the US because contract law is well developed, though as discussed earlier, the basis on which individuals enter into contracts through the consent process is fraught with problems.

While risk assessment is a well-debated concept for companies, the workshop participants highlighted the fact that no similar concept has been formalized for assessing the potential privacy harms to consumers that have occurred or could occur (expected or not) throughout the data life cycle.

The group proposed a structured process by which companies assess the data they collect, and an auditor (public or private) evaluates their collection and retention processes, performs audits and assesses prospective harms to consumers from the company's practices, and makes recommendations for changes. This could be a process open to public comment and scrutiny, including a requirement for auditors to produce a public-facing report. Recommendations could include the deletion of data, design changes or the elimination of certain practices. Based on the outcome of the report, the company would receive some form of certification or assurance of their practices.

This type of process is similar to what happens when legitimate interests are the chosen grounds under the GDPR, and the data processor needs to conduct an ex ante impact assessment before processing the data.

3 Purpose limitation by default

Purpose limitation is the idea that the collection and use of personal data is limited to original intended purpose and that no mission creep occurs. This is a well-defined principle in the GDPR but less so in other jurisdictions.

Taking that concept a step further, if certain harmful types of secondary personal data collection and processing by default (which users otherwise would struggle to understand) are made illegal, individuals are granted an unprecedented level of autonomy over their data collection and processing preferences.

Further, this removes the ability for data collectors to use consent as a basis for engaging in practices that are deemed collectively harmful to society.

4 Positive regulation and responsible innovation

As well as codifying the principle of purpose limitation, companies have a role to play, too.

Inspired by regulatory policy levers such as tax breaks that nudge corporate behaviour, authorities could offer incentives for companies to adopt practices for responsible and ethical data collection and use.

Examples of potential practices could include: refraining from selling or sharing customer data; refusing to use third-party tracking mechanisms on websites or mobile applications; and, germane to this white paper, potentially being pre-certified as compliant in respect of certain legal requirements for the handling of personal data practices if certain conditions are met. Such a model assumes the existence of a supervising regulatory body with the capacity to manage practices, conduct audits and enforce penalties against violators.

Positive regulation can also come from the private sector in the form of an industry-led code of conduct to address data handling practices. Such a model is common in the realm of technical international norm-setting in regards to technical standards, for example.

Regulators could recognize and incentivize the use of a standards model that ultimately is industry-led and continuously updated and signed off on. Perhaps this system could develop into one that allowed more freedom, such as being exempted from future (more robust) Notice & Consent requirements, if certain data practices were met.

5 Privacy by design in smart cities

“Smart cities can coexist with privacy by engaging with the public through a design justice-focused process.

With the implementation of smart city infrastructures, policy-makers are faced with a challenge: the need to provide residents with sufficient notice regarding data collection and a robust consent mechanism to provide them with the means to negotiate their preferences, while also allowing ubiquitous public and private data collection in real time.

Smart cities can coexist with privacy by engaging with the public through a *design justice-focused process*. According to the Design Justice Network,[59] “[d]esign justice rethinks design processes, centres people who are normally marginalized by design, and uses collaborative, creative practices to address the deepest challenges our communities face”.[60]

Additionally, other principles such as transparency are required. Residents of the smart city have a right to know when, where and by whom their personal information is collected and processed.

In addition, residents should have a clear way to signal their consent to – and a clear choice to opt out from – the collection of particular types of data in certain circumstances, such as secondary uses of the data for commercial purposes. For smart cities to operate effectively, the default is akin to opt-in and governments and public authorities rely on legal grounds other than Notice & Consent to lawfully collect and process data from the general public in a smart city environment. Smart cities could also provide residents with particular areas that are effectively surveillance-free – a data-free zone akin to the “airplane mode” on a mobile device. Finally, a design justice approach for smart cities calls for the institution of resident education on issues of data collection and processing, as well as the design of opportunities for local participation – especially for the most marginalized – as key stakeholders in the city’s governance of information flows.

6 Autonomy for tracking in public spaces

Free expression in public spaces is a vital element of an open society. However, generalized surveillance and data collection by both public and private entities in public spaces creates a chilling effect that impedes freedom of expression. Further, obtaining consent from individuals, or providing them with the means to opt-out of either public or private data collection in public spaces is near impossible at this point in history. In the US, this issue has recently grown in significance due to the increase in the number of private surveillance cameras (e.g. Ring doorbells) in areas previously not subject to generalized video surveillance.

To address this issue, an individual’s preferences with regard to the collection and use of their personal data could be designed into a smartphone-based agent or a wearable device, or even, as in the case of the user agent above, be hardwired at digital identity level. Those devices would be designed to communicate, either directly or via a trusted third party (e.g. an electronic communications service), the privacy preferences of the individual to the data collecting entities – whether to a website or a camera on the street, and so on. Thus, data collectors operating in public spaces would collect and process personal data

(including video or other image-based data) in a way that complies with the privacy preferences of the individual. In the absence of prohibitions on the collection of data in public spaces, this approach allows individuals to be able to navigate a world of ambient data collection in real time with minimal disruption to their actual freedom of expression. A caveat to this approach is that the individual's preferences may need to be overridden by the legitimate need to collect personal data in public or private interests, such as functional, security or safety reasons.

7 Data Trusts

Data trusts offer a means by which personal data would be collected and processed in a fair manner. The data trust would be overseen by a trusted authority (appointed in an objective and transparent manner) who could act as the arbiter of and advocate for the personal data rights of the individuals whose data was included in the trust. Accessing a data trust would be contingent upon deciding on the rules of participation by commercial actors or data processors, and on the appointment of the trusted oversight authority.

At present, there is no general consensus as to how to define a data trust. In the UK, interest in data trusts was fuelled by a recommendation from a UK government-commissioned independent review into AI in 2017, which suggested it as a way to "share data in a fair, safe and equitable way".[61]

Globally, there are various ways of defining what a data trust can mean. It can mean a repeatable framework of terms and mechanisms, as defined by the UK AI review, which described data trusts not as a legal entity or institution, but as a set of relationships underpinned by a repeatable framework, compliant with parties' obligations. In practice, this data trust model can potentially specify legal terms and governance processes as well as technical mechanisms of data access.[62]

Another type of data trust is a mutual organization to manage data on behalf of members who have democratic control over the trust and share in its profit. Neil Lawrence, the Director of Machine Learning at Amazon Research Cambridge and Professor of Machine Learning at the University of Sheffield, has suggested that "data subject[s] would pool their data forming a trust, stipulating conditions under which data could be shared … large enough to be effective partners in controlling how [the] data is used".[63] Having a founding constitution and appointed representatives, this type of data trust can take the interests and wishes of the members into consideration to make decisions regarding data sharing and usage. Under this model, there would be aggregated control, which would be delegated to representatives.

Data trusts can also imply a specific legal structure. A trust is a legal structure that enables one party, the trustor, to give another party, the trustee, the right to hold an asset for the benefit of a third party. The beneficiary and trusts have historically been used to hold assets such as property or investments. It has been suggested that data trusts can be used to form a governance in which data is freely given away and data collectors and processors own duties of care and trust to data subjects.[64] The sets of data subjects are the trustors and the beneficiaries of a data trust and the third-party trustees have the duty of decision-making in their best interests, also known as a fiduciary duty. Data trusts have also been described as "civic trusts", an independent, fiduciary governance of third-party data sharing that can review, monitor and enforce ways in which collectors can share data.

Other models of data trusts could also be developed, encompassing or creatively rethinking the characteristics above. For example, one could envisage data trusts as enterprises in the business of providing data management as a service to individuals. Such for-profit fiduciary data caretakers might not necessarily be holding the data themselves, but might, for example, technologically enable the storage of the user's privacy preferences and functioning of personal user agents (described above). They might also assess the data-collecting entities' reputation generally (e.g. by means of own or third-party ratings), facilitating the creation of white or blacklists, against which any request for data might be checked if the user so chooses. Furthermore, such trusted service providers might oversee the data collecting entities' compliance with the individual's legitimate requests and/or offer individuals private or collective legal representation vis-a-vis the data collecting entities.

Another potential solution that addresses these challenges is a community-owned data asset approach. The data custodian must set privacy and security mechanisms that earn trust and securely protect the data. One way to do this is to create a secure logic-controlled data analytics sandbox in which individual-level personal data, which cannot be fully deidentified, is queried by vetted researchers. Researchers would not be able to copy participants' data or otherwise remove data without the explicit permission of the respective data owners to view and/or publish their data. This model could both avoid consent fatigue and enable broad privacy protecting data usage. This approach also addresses the many issues with the institutional sharing of data between countries because the individuals themselves are agents of their respective data at all times.

The various data trust models attempt to provide a solution for people who are not well-versed in privacy jargon and may not necessarily have

time and energy to tailor their decisions on privacy issues. As with any entity that relies on a representative structure, there are concerns with oversight, transparency and accountability. One concern is over how data trusts can truly and faithfully represent the interests and choices of consumers. One way to facilitate the process of incorporating consumer choice into the trust system is to create a method of standardizing risks and benefits. There can be a numerical and standardized evaluation by third-party organizations, and the trusts can adopt policies stating which combinations of risks and benefits they will choose, enabling the consumers to choose the trusts based on their own preferred levels of returns of interests and tolerance of risks. Another potential problem is safeguarding security: If the data trust is the entity that stores and transfer data, how does one create adequate security infrastructures? Whose responsibility is it in the face of a data breach?

8 Algorithmic explainability

When giving consent based on a notice, it is assumed that the notice faithfully explains what will happen with one's data once consent is given. This paradigm breaks down when it comes to "black box" machine learning algorithms: The data processor cannot necessarily foresee or even audit how precisely the algorithm will treat the data in spite of the desired purpose. To assist an individual to exert control over their data in this situation, black box algorithms must be subjected to auditability to limit harm.

If it is impossible to meaningfully deconstruct how a machine learning algorithm arrives at its decisions, then we could take the position that it would be impossible for individuals to provide meaningful consent in any context in which one is deployed. Consequently, it would be necessary to determine the situations or contexts in which black box algorithms are not appropriate.[65] The issue of audits also raises questions about who has the expertise to perform such audits, how auditors will be given access to algorithmic systems, the types of test cases that must be developed to assess their impact and who oversees this entire system.

9 Personal user agents

Autonomous agents are already widely deployed in B2B contexts, and academics have built proofs of concept.

Finally, in line with the smart city example, above, people are typically subject to multiple data collection events on a daily basis. From the hundreds of websites that we may visit to the public and private video cameras that may take our photos in our neighbourhoods, our days are filled with myriad discrete data collection moments. Even when we have genuine intent to affirmatively consent to each moment of data collection, it is practically impossible to do so: No individual has the time to provide affirmative consent on a near-constant basis. This reality arguably undermines our individual agency.

One way to solve this problem would be to create a software-based trusted virtual agent that acts as an intermediary by communicating the privacy preferences of the person to the data collecting entity/technology. Such an agent could also communicate and update personal preferences as the instances of data collection multiply or the terms and conditions change (so that continuous, real-time consent is achievable on behalf of that person). In practical terms, the agent could run on a user's device or be hosted remotely by a third-party trusted service and/or be linked to the user's digital identity.

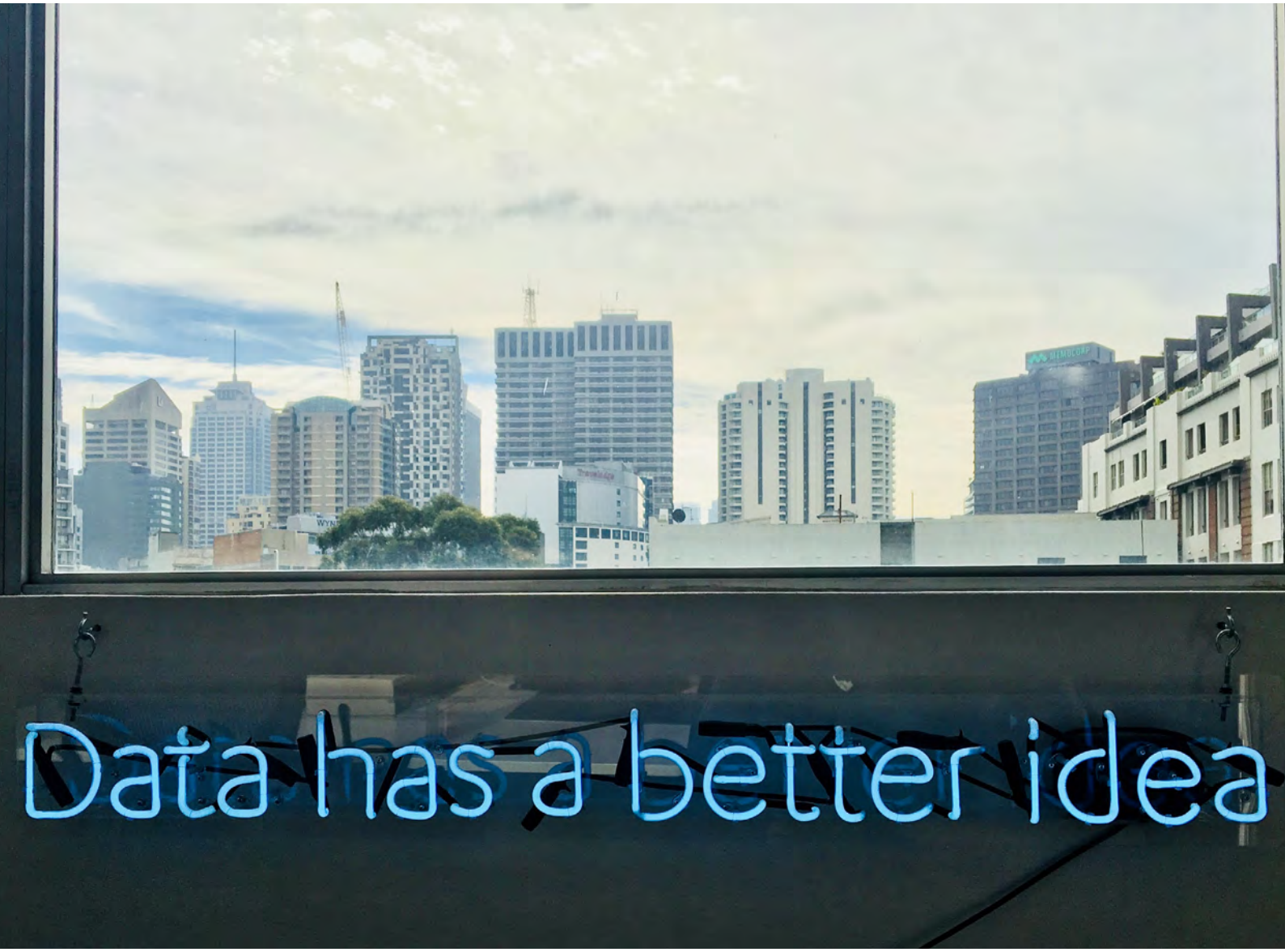
Vital to this approach is the opportunity of the person to preconsent to their preferences. Digital identity offers one such vehicle for consent in the absence, or in lieu, of a browser on a screen.

A trusted virtual agent programmed with the user's preferences could process a privacy policy (the notice) and then act to consent – or not – on the user's behalf. Virtual agents could consult users as appropriate to advise individuals regarding which services they should engage with based on their personal preferences. The trusted agent could act as a trusted filter.

At the most advanced level and given proper technical and ethical development, the agent could act as an adviser, and with appropriate AI capabilities, act dynamically and make practical decisions on behalf of the user, including negotiating trade-offs or compensation with the data collecting entity. There are, of course, safety implications with AI-powered agents and therefore they should be auditable.

This proposal is not new: Various forms of digital agents and other computational methods for negotiating privacy and consent have been proposed and debated for nearly 20 years. However, the complexity of the current and emerging technological landscape, combined with the widespread adoption of smartphones and cloud services (probable platforms for deploying some form of agent), means this idea has come of age and makes it more likely that an agent could successfully be developed and deployed now or in the near future. Autonomous agents are already widely deployed in B2B contexts, and academics have built proofs of concept.[66]

Conclusion



Where to now?

Further research is needed to develop a more nuanced, multipronged toolbox for redesigning and ultimately replacing the notice and consent regime in a way that better empowers people and provides a level of regulatory certainty to businesses so that they can invest in innovation. Businesses have a role to play, too, so the answers lie in a multistakeholder collaborative approach, with the right voices around the table, such as UX designers, including product policy managers, privacy engineers, product technical managers, UX researchers, visual designers and information architects, on the practitioner side, and human-computer interaction scholars, information scientists, anthropologists, and communications and social psychologists on the academic side, to name a few examples.

The current aims of Notice & Consent are worthy, but the execution is outdated in ways that fail to capture meaningful consent when it comes to human-technology interaction.

Given the pace of technological change and the corresponding increase in personal data collection, it is no longer reasonable for people to be expected to signal meaningful consent for all personal data that is processed about them.

In many parts of the world we are now almost perpetually online; the chronic fatigue associated with near-constant consent for data collection and processing is no longer reasonable. People lose the very thing that matters the most when it comes to privacy: control.

There are better ways to ensure that people have a say in what happens to their data. We need to re-examine and reconcile our models of institutional control of collected data to take into consideration personal agency of such information. By taking a human-centred design approach and challenging the reliance on paper-like contracts displayed on screens, we have outlined alternative models for more fit-for-purpose data collection and processing.

It is not a balancing act between human rights and technology, not is it about justifying trade-offs; it is about how to make technology work for people, rather than the reverse.

Sustainable innovation relies on taking a stakeholder approach to avoid systemic risk and optimize outcomes. What happens next is up to those stakeholders.

Exciting experiments are already under way, and we anticipate a proliferation of innovative approaches as the world begins to catch up with the new reality. The key will be to bring policy-makers along for the ride.

This paper is part of a series by the Centre for the Fourth Industrial Revolution focusing on data policy in a post COVID-19 world.

Contributors

Lead authors

Anne Josephine Flanagan
Project Lead, Data Policy, World Economic Forum

Jen King
Director of Consumer Privacy, Center for Internet and Society, Stanford University

Sheila Warren
Head of Blockchain, Digital Assets and Data Policy, and Member of the Executive Committee, World Economic Forum

Contributors

Evîn Cheikosman
Project Coordinator, Data Policy, World Economic Forum

Megan Doerr
Principal Scientist, Governance, Sage Bionetworks

Jana Gooth
Adviser to Alexandra Geese, Member of the European Parliament

Austin Hunter
Former Project Specialist, Data Policy, World Economic Forum

Robert Kain
Chief Executive Officer and Co-Founder, LunaPBC

Andreas Katsanevas
Research Fellow, Consumer Privacy Lab, Center for Internet and Society, Stanford Law School

Caroline Louveaux
Chief Privacy Officer, Mastercard

Ewa Luger
Chancellor's Fellow, University of Edinburgh; Fellow, Alan Turing Institute

Allan Milington
Director, Data Office, EY

Jessica MT Nelson
Project Manager, Canada's Michael Smith Genome Sciences Centre at BC Cancer Agency

m. c. schraefel
Professor of Computer Science and Human Performance, WellthLab, University of Southampton

Fabrice Tocco
Co-Chief Executive Officer and Co-Founder, Dawex

Joe Toscano
Founder, Better Ethics and Consumer Outcomes Network (BEACON)

Alexander Tyulkanov
Deputy Department Director for Regulation of Cyberphysical Systems and Big Data, Skolkovo Foundation

Gabriela Zanfir-Fortuna
Senior Policy Counsel, Future of Privacy Forum (FPF)

Acknowledgements

Rosio Alvarez
Chief Information Officer, Lawrence Berkeley National Laboratory

Laura Brandimarte
Assistant Professor of Management Information Systems, University of Arizona

Pablo Cerdeira
Head, Center of Technology and Society, Fundação Getulio Vargas

Naniette Coleman
PhD candidate, University of California, Berkeley

Lorrie Cranor
Professor of Computer Science and of Engineering and Public Policy, Carnegie Mellon University

Elizabeth Davies
Senior Director, Data Protection, Splunk

Peter Dolanjski
Director, Security and Privacy Products, Mozilla

Margaret Hagan
Director of the Legal Design Lab, Stanford Law School, Stanford University

Alexis Hancock
Staff Technologist, Electronic Frontier Foundation

Natalie Evans Harris
Co-Founder and Head of Strategic Initiatives, BrightHive

Marla Hay
Director, Product Management, Salesforce

Dan Hayden
Data Strategist, Facebook

Jared Ho
Senior Attorney, Federal Trade Commission

Madhu Shalini Iyer
Partner, Rocketship.vc

Meg Leta Jones
Associate Professor, Communication, Culture & Technology Department, Georgetown University

Eddan Katz
Platform Curator, World Economic Forum

Patrick Kelley
Security, Privacy and Anti-Abuse Researcher, Google

Zvika Krieger
Director of Responsible Innovation, Facebook

Monica Lam
Professor, Computer Science Department, Stanford University

Fanyu Lin
Chief Executive Officer, Fluxus

Stefan Lindström
Consul General of Finland in Los Angeles

Jasmine McNealy
Associate Professor, University of Florida

Dena Mendelsohn
Senior Policy Counsel, Consumers Union

Jeff Merritt
Head of Internet of Things, Robotics Smart Cities; Member of the Executive Committee, World Economic Forum

Emilia Porubcin
Center for Internet and Society, Stanford University

Hong Qu
Adjunct Lecturer and Research Director, Harvard Kennedy School

Hannah Quay-de la Vallee
Center for Democracy and Technology

Hannah Ransom
Event and Hospitality Specialist, World Economic Forum

Michael Rubin
Partner, Latham & Watkins

Tomas Sander
Former Data Protection Officer, Director Data Privacy, and Senior Research Scientist in Computer Security, Intertrust Technologies

Mark Schaan
Former Director General, Marketplace Framework Policy Branch, Innovation, Science and Economic Development Canada

Jasmine Yushi Shao
Stanford Law School

Jacob Snow
America Civil Liberties Union of Northern California

Lauren Solomon
Australian Consumer Policy Research Centre

Murat Sönmez
Head of the World Economic Forum Centre for the Fourth Industrial Revolution

Glenn Sorrentino
Principal Product Designer, Salesforce

Anne Toth
Former Head of Data Policy, World Economic Forum

Ron Turner
Chief Technical Officer, XpressRules LLC

Doron Weber
Vice-President, Programs, Alfred P. Sloan Foundation

Lauren E. Willis
Professor of Law, Loyola Law School of Los Angeles

Richmond Wong
PhD candidate, University of California, Berkeley

Editing and production

Alison Moore
Editor

Janet Hill
Head of Editing

Bianca Gay-Fulconis
Graphic Designer

Floris Landi
Lead, Publications and Graphic Design

Endnotes

1. ITU Publications. 2019. “Measuring Digital Development: Facts and Figures”: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf (link as of 17/7/20).
2. We use personal data as defined in the EU’s GDPR for consistency throughout. The US equivalent term is personally identifiable information (PII). For the sake of readability, we conflate the terms as the differences between the two are minor.
3. See generally: Milne, George R., and Mary J. Culnan. 2004. “Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don’t Read) Online Privacy Notices”. Journal of Interactive Marketing: https://doi.org/10.1002/dir.20009; Milne, George R., Mary J. Culnan and Henry Greene. 2006. “A Longitudinal Assessment of Online Privacy Notice Readability”. Journal of Public Policy & Marketing: https://doi.org/10.1509/jppm.25.2.238; Reidenberg, Joel R., Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James Graves, Fei Liu, et al. n.d. “Disagreeable Privacy Policies: Mismatches between Meaning and Users’ Understanding”. SSRN Electronic Journal: https://doi.org/10.2139/ssrn.2418297 (links as of 18/7/20).
4. See generally: Jensen, Carlos, and Colin Potts. 2004. “Privacy Policies as Decision-Making Tools”. Proceedings of the 2004 Conference on Human Factors in Computing Systems – CHI ’04: https://doi.org/10.1145/985692.985752; Turow, Joseph, Michael Hennessy and Nora Draper. 2018a. “Persistent Misperceptions: Americans’ Misplaced Confidence in Privacy Policies, 2003–2015”. Journal of Broadcasting & Electronic Media: https://doi.org/10.1080/08838151.2018.1451867; Turow, Joseph, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley and Michael Hennessy. 2009. “Americans Reject Tailored Advertising and Three Activities that Enable It”. SSRN Electronic Journal: https://doi.org/10.2139/ssrn.1478214 (links as of 18/7/20).
5. See generally: Adjerid, Idris, Alessandro Acquisti, Laura Brandimarte and George Loewenstein. 2013b. “Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency”. In Proceedings of the Ninth Symposium on Usable Privacy and Security – SOUPS ’13, 1. New York, New York, USA: ACM Press.
6. Luger, Ewa, Stuart Moran and Tom Rodden. 2013. “Consent for All: Revealing the Hidden Complexity of Terms and Conditions”. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI ’13). Association for Computing Machinery, New York, NY, USA, pp. 2687–2696.
7. The Usable Privacy Policy Project: https://explore.usableprivacy.org/ (link as of 16/7/20).
8. Kevin Litman-Navarro, “We Read 150 Privacy Policies. They Were an Incomprehensible Disaster”. The New York Times, June 2019: https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html (link as of 16/7/20).
9. schraefel, m. c., R. Gomer, A. Alan et al. “The Internet of Things: Interaction Challenges to Meaningful Consent at Scale.” Interactions, Dec 2017: https://interactions.acm.org/archive/view/november-december-2017/the-internet-of-things (link as of 16/7/20).
10. Egelman, S., J. Tsai, L. F. Cranor and A. Acquisti. “Timing Is Everything?: The Effects of Timing and Placement of Online Privacy Indicators”. In Proceedings of the CHI ’09. ACM, 2009.
11. Adjerid, Idris, Alessandro Acquisti, Laura Brandimarte and George Loewenstein. “Sleights of Privacy: Framing, Disclosures and the Limits of Transparency”. In Proceedings of the Ninth Symposium on Usable Privacy and Security – SOUPS ’13. Association for Computing Machinery, New York, NY, USA, Article 9, pp. 1–11, 2013.
12. User refers to the end user of a service, i.e. the person using the service.
13. Kim, Nancy S. *Consentability: Consent and Its Limits*. Cambridge, UK: Cambridge University Press, 2019.
14. Ibid, p. 15.
15. Ibid.
16. Ibid.
17. Ibid.
18. Ibid, p. 83.
19. Furthermore, it is debatable whether privacy policies themselves are enforceable contracts. See Norton, Thomas B. “The Non-Contractual Nature of Privacy Policies and a New Critique of the Notice and Choice Privacy Protection Model”. 27 Fordham Intellectual Property, Media & Entertainment Law Journal 181 (2016): https://ir.lawnet.fordham.edu/iplj/vol27/iss1/5 (link as of 16/7/20).
20. OECD Privacy Guidelines: https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm (link as of 18/7/20).
21. Hoofnagle, C. *Federal Trade Commission Privacy Law and Policy*. Cambridge: Cambridge University Press, 2016. doi:10.1017/CBO9781316411292 (link as of 16/7/20).
22. The US has federal-level sector-specific laws that cover specific forms of personally identifiable information, namely health data and children’s data, as covered in the Health Insurance Portability and Accountability Act (HIPAA) and Children’s Online Privacy Protection Act (COPPA) respectively.

23. Gellman, R. *Fair Information Practices: A Basic History*, 2019, p 23: https://bobgellman.com/rg-docs/rg-FIPshistory.pdf (link as of 16/7/20).
24. Ibid, p.154.
25. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.
26. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications): https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML (link as of 16/7/20).
27. Zanfir-Fortuna, Gabriela. "10 Reasons Why the GDPR Is the Opposite of a 'Notice and Consent' Type of Law." Future of Privacy Forum, September 2019: https://fpf.org/2019/09/13/10-reasons-why-the-gdpr-is-the-opposite-of-a-notice-and-consent-type-of-law/ (link as of 16/7/20).
28. Solove, Daniel. "Privacy Self-Management and the Consent Dilemma." Harvard Law Review 126, pp. 1880–1903.
29. President's Council of Advisors on Science and Technology (PCAST) Report to the President. Big Data and Privacy: A Technological Perspective. May 2014: https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf (link as of 16/7/20).
30. Hartzog, Woodrow. *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Cambridge, MA: Harvard University Press, 2018, pp. 68–69.
31. Ibid.
32. Kim, pp. 128–129.
33. Kim, p. 124.
34. Frischmann, Brett, and Evan Selinger. *Re-engineering Humanity*. Cambridge, UK: Cambridge University Press, 2018, p. 65.
35. Kim, p. 118.
36. PCAST report, p. 38.
37. While Notice & Consent is just one lawful ground for data processing under the GDPR, and implementation issues are not unique to the GDPR, its influence and importance as a leader in the field of data protection and privacy regulation make it a worthy proxy for how even best-in-class regulation in this area can struggle with the challenge of appropriate implementation given compliance incentives and penalties.
38. Microconsent refers to the concept of granular and seemingly innocuous decision making, so granular that it can become annoying to the user.
39. Norman, Donald, *The Design of Everyday Things*. Cambridge, MA: MIT Press, 2014.
40. Design Kit: The Human-Centered Design Toolkit. Ideo: https://www.ideo.com/post/design-kit (link as of 16/7/20).
41. Norman, Donald. "The Four Fundamental Principles of Human-Centered Design and Application". Jnd.org, August 2019: https://jnd.org/the-four-fundamental-principles-ofhuman-centered-design/ (link as of 16/7/20).
42. See generally: Schaub, Florian, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. 2018. A Design Space for Effective Privacy Notices. *The Cambridge Handbook of Consumer Privacy*: https://doi.org/10.1017/9781316831960.021; Cranor, Lorrie Faith. 2012. "Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice". Journal of Telecommunications and High Technology Law 10; Kelley, Patrick Gage, Joanna Bresee, Lorrie Faith Cranor and Robert W. Reeder. 2009. "A 'Nutrition Label' for Privacy". Proceedings of the 5th Symposium on Usable Privacy and Security – SOUPS '09: https://doi.org/10.1145/1572532.1572538; Kelley, Patrick Gage, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. Standardizing Privacy Notices. Proceedings of the 28th International Conference on Human Factors in Computing Systems – CHI '10. https://doi.org/10.1145/1753326.1753561 (links as of 16/7/20).
43. The GDPR requires opt-in only.
44. In the US, improvements to the design of privacy policies of platform giants such as Google or Facebook have been in response to settlements with the Federal Trade Commission. Companies that attempt to make privacy a core aspect of their business often have better designed (and more legally straightforward) privacy policies, such as DuckDuckGo, Brave and others.
45. Article 6 of the GDPR offers six lawful grounds for personal data processing, including Notice & Consent. The other five are: performance of a contract, compliance with a legal obligation, vital interest, public interest and legitimate interest.
46. Kim, *Consentability*, p. 99.
47. Platform for Privacy Preferences (P3P) Project: https://www.w3.org/P3P/ (link as of 16/7/20).
48. Cranor. "Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice".
49. Ibid.
50. The INTUIT Project: https://intuitproject.org (link as of 16/7/20).
51. Luger, E., S. Moran and T. Rodden. 2013. "Consent for All: Revealing the Hidden Complexity of Terms and Conditions". In Chi '13: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM Press.

52. Bellotti, V., and A. Sellen. 1993. Design for Privacy in Ubiquitous Computing Environments. In Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17, September 1993, Milan, Italy ECSCW '93: https://link.springer.com/chapter/10.1007/978-94-011-2094-4_6 (link as of 16/7/20).

53. Richards, Neil M., and Woodrow Hartzog. "Taking Trust Seriously in Privacy Law". 3 September 2015. 19 Stanford Technology Law Review 431 (2016).

54. Taylor, L. 2017. "What is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally". Big Data & Society: https://journals.sagepub.com/doi/full/10.1177/2053951717736335 (link as of 16/7/20).

55. The Consentful Tech Project: https://www.consentfultech.io/ (link as of 16/7/20).

56. Planned Parenthood, "Sexual Consent": https://www.plannedparenthood.org/learn/relationships/sexual-consent (link as of 22/7/20).

57. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1888-1-1 (link as of 16/7/20).

58. Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (link as of 16/7/20).

59. The Design Justice Network: https://designjustice.org/ (link as of 16/7/20).

60. The full set of principles are available at: https://designjustice.org/read-the-principles (link as of 16/7/20).

61. What Is a Data Trust? Open Data Institute: https://theodi.org/article/what-is-a-data-trust/#1527169770610-7c7f3670-046362d2-2d92 (link as of 16/7/20).

62. Ibid.

63. Lawrence, Neil. "Data Trusts Could Allay Our Privacy Fears." The Guardian, June 2016: https://www.theguardian.com/media-network/2016/jun/03/data-trusts-privacy-fears-feudalism-democracy (link as of 18/7/20).

64. Edwards, Lilian. "The Problem with Privacy." 3 June 2004. International Review of Law Computers & Technology, 18(3), pp. 263–294, November 2004: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1857536 (link as of 16/7/20).

65. To some extent, the GDPR has done this; see Article 22, *Automated Individual Decision-Making, Including Profiling*.

66. See, for example: Baarslag, T., E. H. Gerding, R. Aydogan and m. c. schraefel. "Optimal Negotiation Decision Functions in Time-Sensitive Domains." 2015 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT), Singapore, 2015, pp. 190–197; Baarslag, Tim, Alan Alper, Richard Gomer, Muddasser Alam, Perera Charith, Enrico Gerding and m. c. schraefel. 2017. "An Automated Negotiation Agent for Permission Management." In AAMAS 2017: Proceedings of the 16th Conference on Autonomous Agents and MultiAgent Systems. ACM. pp. 380–390. Baarslag, Tim , Alper T. Alan, Richard C. Gomer, Ilaria Liccardi, Helia Marreiros, Enrico H. Gerding and m. c. schraefel. 2016. "Negotiation as an Interaction Mechanism for Deciding App Permissions. In Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA '16)." Association for Computing Machinery, New York, NY, USA, 2012–2019.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
contact@weforum.org
www.weforum.org