Building Consentful Technologies

1. What does consent have to do with technology?

A lot of us know about consent with regard to our physical bodies, like in the context of medical decisions or sexual activities. But when it comes to our digital lives, there's a lack of discussion about what consent means for our data, our identities, and our online interactions.

This zine is intended for anyone who uses, makes, or is affected by digital technologies and wants to build a more consentful world. It is by no means a comprehensive resource, but rather a collection of thoughts and questions we've gathered in the hopes of growing this conversation.

1.1. Content warning

We've tried as much as possible not to reproduce harm and violence in this zine, however we do make several references to sexual violence. We have used [this symbol] at the top of the relevant pages to indicate where this content appears.

1.2. Consent in the dictionary

Consent /kənˈsent/
Noun: Permission for something to happen or agreement to do something.
Verb: Give permission for something to happen

2. Who wrote this?

This zine was written by Una Lee and Dann Toliver, who are the team behind the Ripple Mapping Tool. Una is a design practitioner, a collaborative design facilitator, and a design justice advocate. Dann spends a lot of time talking to people about computers, and to computers about people.

3. Consentful technology is about having control over our digital bodies

When it comes to our physical bodies, we know there is more to consent than a simple yes or no. Medical procedures like surgery require the informed consent of the patient — they must be aware of both the benefits and risks in order to really consent. With sexual activity, if someone says yes to one form of intimacy but is coerced into performing another, the sex is not consensual.

But what about consent beyond our physical bodies? These days, we also have digital bodies. Digital bodies are made up of pieces of personal data. Like our physical bodies, our digital bodies exist in relationship with others and can participate in communities. They can also experience harm. Although the harm to them might not be physical, our digital bodies are frequently acted upon in non-consensual ways:

- Apps like Uber track our location even when we are not using them
- Unchecked threats of sexual assault in digital spaces like Twitter
- “Doxing” — distributing a target's private information, like their social network account passwords
- “Revenge pornography” — posting intimate images without the subject’s consent
- Private information such as biometric data being shared across government databases, which particularly impacts immigrants, people with disabilities, and the poor.

With our digital bodies, there is also more to consent than a “yes” or “no.” As our physical bodies become increasingly interlinked with our digital bodies, harm can’t be prevented by trying to avoid technology. And harm can’t be justified because someone checked a box that said “I agree to these terms and conditions.”

Instead, cases like those on the previous page point to a need for a cultural and technological shift in how we understand digital consent, as well as a political shift in how we advocate for control over our digital bodies. We want to offer up the idea of consentful technologies to help us move toward this. Consentful technologies are applications and spaces in which consent underlies all aspects, from the way they are developed, to how data is stored and accessed, to the way interactions happen between users.

We use consentful instead of “consensual” because the latter implies a singular ask or interaction. Consentful technology is about a holistic and ongoing approach to consent.

What is a digital body?

Digital bodies are like physical bodies in that they’re comprised of smaller bits. Instead of cells and organs, digital bodies have data and metadata.

However unlike a physical body that exists in one place, our digital bodies are scattered throughout the servers that make up the internet. Also unlike physical bodies, our body parts are controlled exclusively by the environment they live in. What would a future look like in which the cells of our digital bodies have more autonomy?

3.1. Understanding consent is as easy as FRIES

For the sake of starting with a common but robust definition of consent, we turn to Planned Parenthood’s FRIES acronym.[1]

- **Freely given.** Doing something with someone is a decision that should be made without pressure, force, manipulation, or while incapacitated. In technology, if an interface is designed to mislead people into doing something they normally wouldn’t do, the application is not consentful.

[1] Adapted from Understanding Consent is as Easy as FRIES, Planned Parenthood.

- **Reversible.** Anyone can change their mind about what they want to do, at any time. In technology, you should have the right to limit access or entirely remove your data at any time.
- **Informed.** Be honest. For example, if someone says they'll use protection and then they don't, that's not consent. Consentful applications use clear and accessible language to informs users about the risks they present and the data they are storing, rather than burying these important details in e.g., the fine print of terms & conditions.
- **Enthusiastic.** If someone isn't excited, or really into it, that's not consent. If people are giving up their data because they have to in order to access necessary services and not because they want to, that is not consentful.
- **Specific.** Saying yes to one thing doesn't mean they've said yes to others. A consentful app only uses data the user has directly given, not data acquired through other means like scraping or buying, and uses it only in ways the user has consented to.

How might we expand this definition to address the intangible and networked qualities of digital technologies?

4. Consent makes technology more just and equitable

Think of a technology you use on a day to day basis. Can it have unjust or inequitable impacts on anyone? Who owns the technology, and who participates in the making of it?
In a lot of cases, you'll find that those who might experience harm such as harassment or surveillance are not the owners of the technology. Sometimes there is overlap between those who work on the building of the technology and those who could be harmed, but often there isn't.

There are many ways to make technology more just and equitable, and consent is one important consideration. Non-consentful features and interactions can be minor nuisances for some people, but can be very harmful to others. When Facebook introduced photo tagging, anyone could tag you in a photo, whether or not you were okay with it. For some users, that could lead to embarrassment if the photo wasn't particularly flattering. But for other people, the harm could be much more serious. For trans users, tagging photos from their pre-transition lives without their consent could lead to them being outed, which can have consequences for employment, housing, safety, and more.

In response to user outcry, Facebook eventually implemented a process by which users can approve tagged photos. However, it required a critical mass of complaints to make this happen. And, Facebook still stores photos that are tagged with your face in its database, which informs its facial recognition algorithms. Whether you consented to being tagged or not, Facebook has a 98% accurate idea of what your face looks like.[2]

---

[2] Facebook's image recognition algorithms can "recognize human faces with 98% accuracy, even if they [aren't] directly facing the camera...[It can] identify a person in one picture out of 800 million in less than five seconds." 'Inside Facebook's Biggest Artificial Intelligent Project Ever,' Fortune Magazine, April 13, 2016.

Consider the technology you were thinking of earlier. What would it look like if it was built to ensure that everyone had an equitable experience, and some users were not negatively impacted more than others? Who would need to own and build the technology for this to happen?

Building consentful technologies together

It can be hard for people who aren't developers or investors to imagine how they can be involved in building consentful tech. It can also be challenging for the people involved in making technology to imagine how to center their work around people who are most vulnerable. But we all have important roles to play.

Non-technology folks can contribute to building consentful tech by:

- Holding the platforms we use accountable to how they use our data
- Advocating for consent-focused policy and legislation
- Intervening in development processes through community organizing (petitions, demonstrations, etc.)
- Signing on to platforms that are consentful
- Learning more about code, policies, and legislation

Tech folks can contribute to building consentful tech by:

- Advocating for diverse teams
- Opening up design & development processes to people who those who are vulnerable to harm
- Working towards a culture of consent in our companies and organizations
- Mentoring newcomers, particularly those who are often excluded or marginalized from mainstream tech communities
- Growing our knowledge on concepts like collaborative design processes and intersectionality
- Consistently reviewing our development processes

4.1. What this zine builds upon

Our thinking around consentful technology has been shaped by numerous other ideas. This zine builds upon the following concepts and movements:

4.1.1. Consent culture

The anti-violence against women movement has given us the concept of consent culture. Consent culture is "a culture in which asking for consent is normalized and condoned in popular culture. It is respecting the person's response even if it isn't the response you had hoped for. We will live in a consent culture when we no longer objectify people and we value them as human beings. Consent culture is believing that you and your partner(s) have the right over your own bodily autonomies and understanding that each of you know what is best for yourselves."[3] We believe that consentful technology has an important role to play in creating a consent culture.

---

[3] Only with Consent.

4.1.2. Design Justice

Design justice is an approach to design that is rooted in equity and community. The Design Justice Network is “striving to create design practices that center those who stand to be most adversely impacted by design decisions in design processes.”[4] Design processes that are led by and centered around people who can be unjustly impacted by technology are a cornerstone of consentful tech.

4.1.3. Digital Justice

According to the Detroit Digital Justice Coalition, "communication is a fundamental human right. We are securing that right for the digital age by promoting access, participation, common ownership, and healthy communities.”[5] Consentful technology is modelled on equitable access, participation in the design process, ownership and control of our digital bodies, and communities based in consenting interactions.

4.1.4. Community Technology

The Detroit Community Technology Project defines community technology as "a method of teaching and learning about technology with the goal of restoring relationships and healing neighborhoods.”[6] Consentful technology builds healthy digital communities through consenting interactions and relationships.

5. Consent from the ground up

How might the technologies we are most reliant upon look if they were designed with consent at their core? What if, before writing a single line of code, the following questions were asked:

- Are people **Freely** giving us their consent to access and store parts of their digital bodies? Can potentially harmful personal information about a person be displayed or stored without their consent?
- Does our system allow for **Reversible** consent? How easy is it for people to withdraw both their consent and their data?
- How are we fully and clearly **Informing** people about what they’re consenting to? Is important information about the risks a user might be exposed to buried in the fine print of the terms & conditions?
- How are we making sure that the consent is **Enthusiastic**? Is there an option not to use this technology, which means that people use it because they prefer to use it? As we've said before, in many places one can only access social service benefits online. Declining to register with these online services is not an option for those who need these benefits most.

---

[4] Design Justice Network.

[5] Detroit Digital Justice Coalition.

[6] Detroit Community Technology Project, Teaching Community Technology Handbook.

- Can people consent to **Specific** things in this system and not others? Can people select which aspects of their digital bodies they want to have exposed and have stored?

When technology is built without asking these questions from the beginning then serious harm can happen, and it often takes multiple instances of harm for a patch to be designed. Popular photo and video sharing platforms, for instance, have been used to circulate images of acts of sexual violence, which re-harms people who have experienced violence and perpetuates violence in our culture. It is extremely difficult to delete these images once they have been distributed.

These are obviously not the use cases the developers and owners of these platforms were intending, but they do illustrate the harm that can happen when we fail to design with consent in mind from the ground up, and foreground the concerns of users who could be severely and unjustly impacted.

We can and must do better.

5.1. Dealing with risk

Unlike our physical bodies, a digital body can be in many places at once. It can be at rest in a database, socializing in the cloud, or traveling through the tubes. You should have a good understanding of the risks to your digital body that are involved in its activities, so you can make informed decisions, just like the decisions you make about where to travel, where to stay, and how to get there with your physical body.

Historically speaking, technology providers have done a poor job of acknowledging those risks. We see this in data breaches, where intimate details of digital bodies (passwords, credit card information, medical information, private photos etc) are exposed publicly or sold to the highest bidder. We also see it in cases where companies make use of your digital body in ways you didn't intend, and whether that's malicious (using your profile pic to advertise dating services) or seemingly benign (adding a new feature that exposes you to additional risk) it is still an act taken upon part of your digital body without your consent.

We can do better. By designing the system so certain things are impossible, we lower the trust barrier for that system. For example, your personal information could be stored encrypted, with the decryption keys residing only on your own devices. The application sends data and code to your device, and your consent is requested for each operation.

If we can't make it safer then we can acknowledge the remaining risks and educate users about them. Let's build industry standards for reporting risks at rest, in transit and during processing. Additional standards for functionality-based risk would help too. This is a big problem: it requires software developers, industry groups, advocates and users all working together, and it starts by having this conversation. Let's talk about how risky it currently is to use software, and how we can make it safer and more accessible for everyone.

5.2. Ideas for technical mechanisms

A technique called **differential privacy**[7] provides a way to measure the likelihood of negative impact and also a way to introduce plausible deniability, which in many cases can dramatically reduce risk exposure for sensitive data.

Modern **encryption techniques** allow a user's information to be fully encrypted on their device, but using it becomes unwieldy. Balancing the levels of encryption is challenging, but can create strong safety guarantees. **Homomorphic encryption**[8] can allow certain types of processing or aggregation to happen without needing to decrypt the data.

Creating **falsifiable security claims** allows independent analysts to validate those claims, and invalidate them when they are compromised. For example, by using subresource integrity to lock the code on a web page, the browser will refuse to load any compromised code. By then publishing the code's hash in an immutable location, any compromise of the page is detectable easily (and automatically, with a service worker or external monitor).

Taken to their logical conclusion these techniques suggest building our applications in a more **decentralized**[9] way, which not only provides a higher bar for security, but also helps with scaling: if everyone is sharing some of the processing, the servers can do less work. In this model your digital body is no longer spread throughout servers on the internet; instead the applications come to you and you directly control how they interact with your data.

6. Consent is an ongoing process

The process of asking for consent does not stop at the first yes. Saying yes to an interaction once — whether it's a hug or linking your user account with your Facebook profile — should not imply that the consent was provided for an indefinite period of time.

Platforms like Google are incorporating periodic check-ins with users about what they've consented to, which is a good start. But Google's account holders aren't the only ones impacted by non-consent on their platform: for example, anyone who has their name and email address added to an open Google Sheet has potential exposure.

This is because many of the technologies we rely on only require the consent of a user to the system, or of users to each other. What about people who are impacted who are not users? We have found that asking people directly, as one would in a physical interaction, is a strong practice. How might your experience of the Internet shift if people who had access to your digital body, whether in the form of photos or contact information, were to check in with you from time to time about it? What technologies would we need to build to help us manage ongoing and direct consent processes?

---

[7] The Algorithmic Foundations of Differential Privacy (2014), Cynthia Dwork and Aaron Roth.

[8] A Fully Homomorphic Encryption Scheme (2009), Craig Gentry.

[9] Scuttlebot.

Pullquote: “Is it cool if I Snapchat this video of you dancing with that hot dog?”

6.1. An equitable iteration process

“Fail faster” is a maxim of application developers these days. It means putting something out into the world quickly and responding to user feedback in future iterations. This is a great way to optimize the value of your application to your users, by starting with something simple and experimenting until you get the right features.

Unfortunately while this process can increase positive impacts, it does nothing to diminish negatives impacts. The fail faster approach experiments not only with features but also with the lives of people using those features. Consider the release of the Alexa app for Amazon Echo, which did not allow for blocking calls or texts. This raises immediate red flags for anyone who has been doxxed or stalked, and may have directly lead to harm for Alexa users.

It isn’t enough to iterate features in response to harm -- we must also iterate the process that lead to those features being released. What would that process look like if it was centered around the privacy and security of survivors of violence? Of people from communities that are regularly subject to state surveillance?

7. Consentful technology relies on community and accountability

We have talked a lot about what we can do to build more consentful technologies. But implementing these measures can’t guarantee that non-consensual actions will not happen. This is why community and accountability are critical in addressing harm.

Digital communities

More and more, our digital bodies exist in digital networks and communities. Whenever there are multiple relationships between people, a type of community or network is created. One type is formed when people sign up for a service — as users, they are now in relationship with whoever owns and works on the technology. Another type of community is created when users interact with each other. Digital communities can overlap with physical communities.

Accountability means being held responsible for your actions. The accountability mechanisms available in most technologies are not good enough. Blocking users who are harassing you does not easily stop them from harassing others. Reporting an image that is harmful to you does not stop that image from being posted by others and to other platforms.

Our digital bodies interact with each other, intermediated by the servers they inhabit. Currently all the control is in the environment, and the data that makes up our digital bodies is passive and lacks agency. By binding that data into a cell with its own logic, protected by encryption, we could restore autonomy to our digital bodies, allowing interactions to involve us instead of acting upon us.

7.1. A Community Accountability Approach

Some people have called for police departments to become more knowledgeable about current technology, and for lawmakers to create harsher punishments for people who are committing violence online. But the problems with this approach mirror those that are rampant in enforcement of sexual assault laws. Often it is the person who experienced the harm who is blamed - why did you send nude photos to your ex, or why didn't you just ignore that troll? And, for Black and Indigenous people, racialized immigrants, LGBTQ people and more, police and prisons are key vectors of violence in daily life.

What if we built community-based responses to harm and violence into our technologies? When we act harmfully against others, whether it is intentional or not, there is an impact on both that person and the community as a whole. This is true whether the harm is interpersonal or caused by algorithms. So we must be responsible to each other as individuals as well as members of a community. This is what is meant by community accountability.

"Community accountability is a community-based strategy, rather than a police/prison-based strategy, to address violence within our communities. Community accountability is a process in which a community — a group of friends, a family, a church, a workplace, an apartment complex, a neighborhood, etc — work together to do the following things:

- Create and affirm values & practices that resist abuse and oppression and encourage safety, support, and accountability
- Develop sustainable strategies to address community members' abusive behavior, creating a process for them to account for their actions and transform their behavior
- Commit to ongoing development of all members of the community, and the community itself, to transform the political conditions that reinforce oppression and violence
- Provide safety & support to community members who are violently targeted that respects their self-determination"6

What would a community accountability approach to digital communities look like? How would it work for both people who are users of the technology in question, as well as people who might be impacted by it? How could this change the way that the creators of algorithms are held accountable for the harms that their biases cause?

7.2. Strong communities give rise to more consentful technologies

When attention is paid to relationships, stronger communities result. This is the case in physical communities as well as digital. Users and makers can strengthen their communities and improve consent therein by asking:

- How can we better protect each other? For example, is there a technical way to have other community members see and respond to harassing messages, so the person who is targeted does not have to deal with the barrage alone?
- How can we hold each other accountable as a community? What are some community-based strategies for addressing non-consensual actions that work on the roots of the issue?

- How can we better support and uplift each other? How can we normalize asking for consent on our platform?

Small changes can make a big difference when we add a little friction to pathways used for abusive behaviour, and when we make it easier for people to help each other. For example, new users might have a quieter voice until they've been around awhile, or messages mentioning you could be downvoted by your friends so you won't see them.

8. Consentful technology moves us towards consent culture

Currently, achieving some measure of privacy and security in technology requires active participation from users, which means when that trust is violated it is the users who pay the price, and often the users who are blamed. The cost of interacting with technology securely is quite high, and those least able to pay that cost are also those most at risk of harm when things break. Just as we should not blame survivors for sexual violence, we must not place the burden of safety on users in terms of who is responsible and who suffers the consequences.
We see an alternative to this in consent culture. Consent culture is a culture in which asking for consent permeates all our interactions small and large — whether it's asking before going in for a hug, checking in about taking a photo, or asking whether a sexual activity feels okay. With technology mediating so many of our daily interactions, it plays an increasingly large part in establishing the type of culture we live in. Building consentful technology is not just about our applications and data; it is about creating a culture of consent for the entire world to share in.

9. Resources

Readings

- Consent of the Networked: The Worldwide Struggle for Internet Freedom Rebecca MacKinnon. Lebanon, IN: Basic Books, 2012.
- Design Justice Zine, Design Justice Network.
- Our Data Bodies Project 2016 Report, From Paranoia to Power.
- Learning Good Consent: On Healthy Relationships and Survivor Support. Edited by Cindy Crabb. Chico, CA: AK Press, 2016.
- Teaching Community Technology Handbook, Detroit Community Technology Project.

Orgs & Projects

- Crash Override Network
- INCITE!
- Hold Your Boundaries project
- Troll Busters

10. Acknowledgments

This zine would not exist without funding and moral support from the Mozilla Foundation and Allied Media Projects. Much gratitude to the extended Allied Media Conference family for generously lending your time and insights about consent. Thanks to Shameela Zaman, Lupe Pérez, Hisayo Horie, Erin Toliver, Tyler Sloane, and Alex Leitch for reviewing the content of this zine. Thank you also to the Difference Engine Initiative participants — you were the spark that inspired this all.

Graphic Design: And Also Too
Logos: Mozilla Foundation, AMP, And Also Too

Feedback?

We welcome your comments on this zine. To send feedback, please fill out our Google form.