ARTICLES > INTERVIEW

Creating a Culture of Consent for Our Digital Future: A Conversation with Tawana Petty

By: Tawana Petty, Ever Bussey

MOVEMENTS & MOBILIZATION

Bussey, Ever, and Tawana Petty. "Creating a Culture of Consent for Our Digital Future: A Conversation with Tawana Petty." Just Tech. Social Science Research Council. March 6, 2024. DOI: https://doi.org/10.35650/JT.3066.d.2024.

With support from the Benton Institute's Opportunity Fund Fellowship, Greta Byrum (Benton Institute Fellow) and Ever Bussey (Just Tech Program Officer) interviewed community organizers, hacktivists, and cyber security experts to learn about the threats that face new digital adopters and how their work effectively mitigates these harms. With the consent of the interviewees, we are happy to share these conversations in hopes that you can learn to manage this historic push for internet adoption.

In their conversation, Bussey and Just Tech Fellow Tawana Petty discuss how data extraction and surveillance impact marginalized communities, working with policymakers, and how to address the proliferation of artificial intelligence in an inclusive and consentful manner.

Tawana Petty is a 2023–2025 Just Tech Fellow. She is a social justice organizer whose work focuses on racial justice, equity issues, water rights advocacy, data privacy, and consent. Based out of Detroit, she is also the founding director of Petty Propolis, a Black women-led artist incubator and social justice organization that teaches writing and antiracism workshops, hosts artist retreats, and organizes an artist festival in historic Idlewild, Michigan.

Ever Bussey (EB): In a couple of sentences, could you describe the online privacy, security, and safety training and preparedness work you do? Who is it directed toward and why?

Tawana Petty (TP): I don't consider myself a person who trains on those types of things like online privacy or cybersecurity. However, through my work with Detroit Digital Justice Coalition, over the past decade, we have convened DiscoTechs, short for Discovering Technology fairs. We encourage using tools

from organizations like Equality Labs or consulting the expertise of digital security trainers like Sarah Aoun or Matt Mitchell. Those are folks whom I would consider to have expertise around online safety and how we secure our digital tools. My work focuses on trying to foster a culture of consent and to push for the opportunity to opt out of systems and give away our data, or to take time to read particular privacy policies, with the understanding that they aren't always super accessible. So, we try to break them down as much as possible. I consider myself more of a culture shifter who focuses on how to rethink our relationship how with these systems, rather than a person who teaches online security.

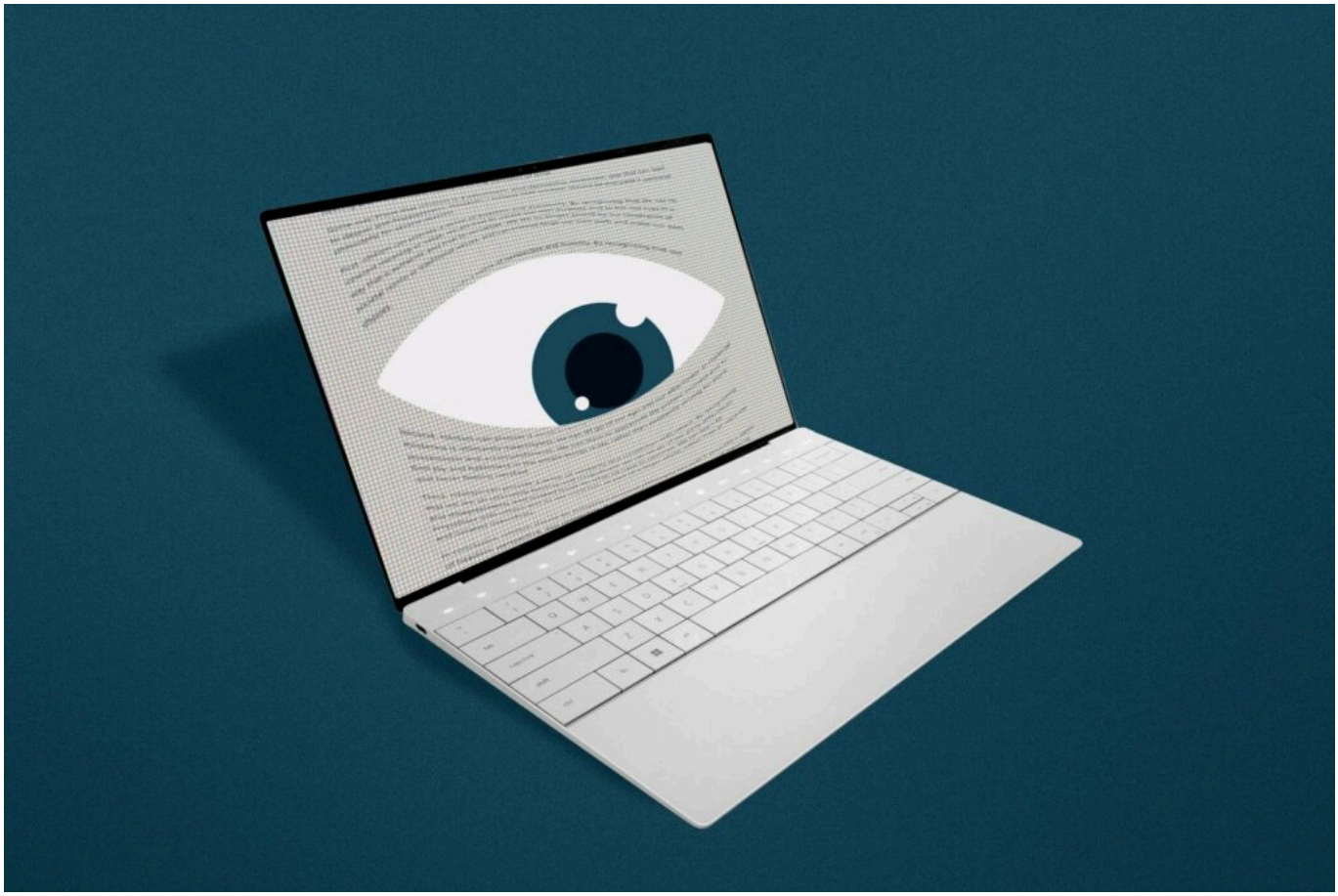
EB: Why is shifting the culture around our relationship with online consent important? Why are you interested in doing that work? And who is it for?

TP: I'm interested in doing that work because I recognize how pervasive dominant narratives are. In this work, specifically the work that I've been engaged in around data justice and digital justice, a lot of folks have been coerced into a mindset of powerlessness where they're like, "Well, they have our stuff anyway," or "They're already going to take this." I've learned that the more you encourage people that we still have a voice in the matter, the more folks tend to push back against systems that are unjust. And it doesn't have to be a given that your data is going to be extracted and weaponized against you. We still have opportunities to mount a resistance against systems that are harmful. To me, those people are the general public. They're anybody who is exposed to any type of system that's extracting our data. However, I do prioritize Black folks in my work.

EB: Why Black folks? Say you're talking to me and I'm one of the people that's just throwing my hands up in defeat. Why should I be concerned about something like that? What do I stand to lose?

TP: There's a lot to lose. I always tell people who say, "I have nothing to hide," or "They have everything about me anyway," that there's always something to hide. Just think about being in your apartment on any given day and the government or a tech company is able to see everything that you do inside your apartment without your consent. That's the way we have to operate. We have to think about those moments of privacy that are being eroded and how our data and information are being leveraged to target us to be consumers of systems, not producers of systems, and how agencies like law enforcement have leveraged our data to create predictive policing systems or to hypersurveil communities. We're looking at systems that are systemically racist.

That's a reason why I prioritize Black people, because we are some of the most harmed by these systems, whether it's housing, law enforcement, education, or the medical industry. All of these institutions and corporations use massive amounts of data to make decisions about our lives. When they do that, they're doing it from a racially inequitable lens. We not only have a responsibility to push back on those types of systems, but it's the only way that we're going to be seen as fully human and not have systems that become artificially intelligent and hyperracist on levels that move even swifter than the human aspects of racism.



EB: If you had to pick one or two threats to prepare for, which of the following do you think is most important to the people you work with? Data privacy, protection against fraud or hacking, online harassment or threats, surveillance and discrimination, or something else.

TP: Oh, my goodness, it's hard to pick. But I would say surveillance for sure, because the people who are being hypersurveilled are already the most marginalized. We're rapidly moving toward a social credit system in which the populations deemed undesirable are the ones being contained within these overly surveilled communities. While folks who have greater wealth and are white have more opportunities to move about freely, to have upward mobility, more and more Black communities are being hypersurveilled, being squeezed out of systems, and are having our civil liberties and human rights eroded.

Surveillance is a very prevalent harm that I am witnessing and can see being exacerbated. Then, I would say, secondly, fraud targeting our senior citizens who are very vulnerable to deep fakes and other types of replications of our voices and data. They are being spammed in ways that allow access to their bank accounts and other private information. The proliferation of online data access and manipulation using artificial intelligence is going to be a pretty great risk for those folks who are not literate in these systems and most times that's going to be our elders in the community. Although, I would also argue we are all vulnerable to a degree.

EB: From your experience working with specific community groups, what should government officials know about what's at stake if internet security and safety concerns are not addressed?

TP: I would just reiterate those two. I think government officials should know (1) these examples are not the end all be all, but I do think government agencies should prioritize the principles in the Blueprint for an AI Bill of Rights. I know it's not a governing document, but at the very least it has human alternatives, and it has all of these opportunities to make sure that we're trying to challenge algorithmic discrimination. I think that that should become a systemic policy throughout agencies, and there should be particular emphasis on making sure that law enforcement agencies do not have exemptions that allow them to evade the principles.

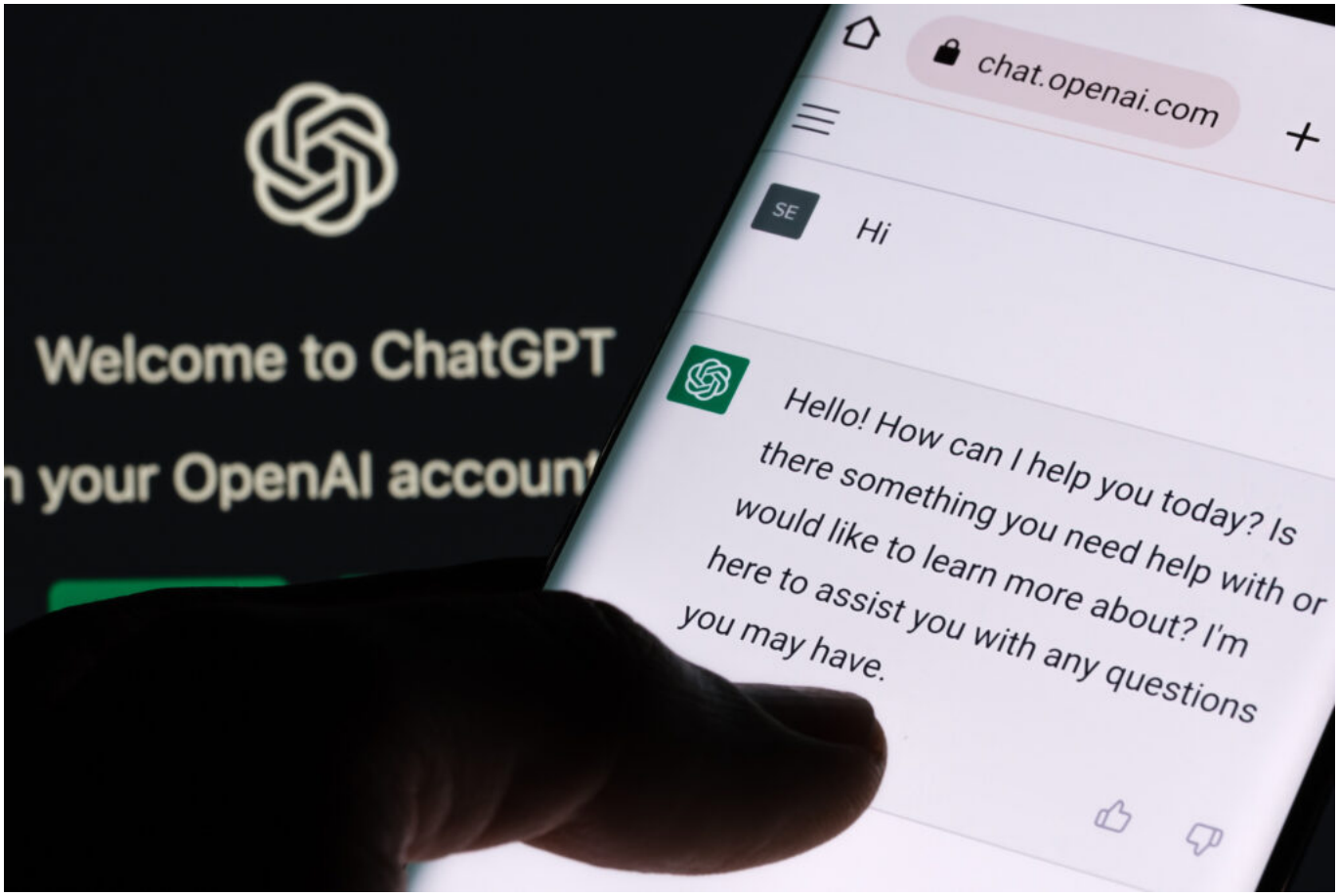
I would say systematizing the five principles identified in the Blueprint and intentionally addressing the clearly defined ways that the National Institute of Standards and Technology's (NIST) AI Risk Management Framework defines computational, statistical, and human cognitive biases, as well as implementing President Biden's Executive Order on Further Advancing Racial Equity and Support for Underserved Communities as well as his Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence are good starts at addressing some of my concerns. However, there are still lingering tensions around the ways that law enforcement agencies seem to be exempt from systemic change. I think with the rapid proliferation of artificial intelligence in our lives, it would be a mistake not to put some serious guardrails on its use by law enforcement. We have learned a lot from the negative impacts of facial recognition misidentifications and the harms of predictive policing on communities of color. I think the move to push us into AI trustworthiness without consent, transparency, and true accountability is a mistake.

EB: If I were a government official and you want to give me an example, something specific and tangible about how people need to prepare for the impending privacy or surveillance threats as more people get online, could you share one?

TP: I would use OpenAI and ChatGPT, not even just ChatGPT, but all of their large language model (LLM) related systems. I would say that we are learning a lesson right now about what happens when massive amounts of data are extracted from our communities with little transparency. We are also experiencing the negative impacts of the rapid proliferation of disinformation. This is especially harmful during election seasons. We are also limited in the ways we can challenge the harms created by the spread of misinformation through so-called "hallucinations." I'm struggling with what to say, because I don't want to use the same language they use. ChatGPT is being marketed, despite its proven harms, as some kind of autonomous nonhuman connected system that's making all these mistakes, which minimizes who can be held accountable for those mistakes. I think we're sitting at a moment now for policymakers to hold actual individuals and entities accountable for the harms that these systems are creating and not fall into the hype that makes it seem like there's just some rogue technology out here lying to everybody without human contribution from the tech companies who have unleashed this upon our public.

History has shown us that the public will be the driving force for change, if the companies and the government do not make moves to reduce real harm. We are already seeing class action lawsuits, protests, and boycotts. People are fed up with the lack of transparency, not knowing what their data is being used for, how it's being used, who it is being shared with, or what impact it's having on our communities. I would say policymakers should really take this moment to dissect what is happening, and

how we got this far without regulations put in place. We've got to stop letting tech companies just pay out dollars that have little impact on their bottom lines, while they continue to create harm. Yes, they should financially pay for their harm, but they must also move to reduce it. We have to use the Framework, the Blueprint, and the Executive Orders to identify which principles and guidelines are being violated by these companies and hold them accountable. As the public, we also have to make sure that the government practices what it preaches. They cannot be exempt from the principles and guidelines they espouse when they procure and leverage these same technologies.



ChatGPT chat bot screen seen on smartphone and laptop display with Chat GPT login screen on the background. A new AI chatbot by OpenAI. Stafford, United Kingdom, December 13, 2022.

EB: Who represents a threat and why? So, for instance, regarding data privacy and the extraction of our data, who should we be concerned about and why? Is it corporate, state, or nonstate actors?

TP: It's definitely corporate, state, and nonstate actors, because there is limited regulation. I never thought I would be a person who was touting regulation and enforcement, but I've seen the harms of not having consistent regulation and enforcement in place. I'm at the point now where I find myself championing enforcement by the Federal Trade Commission (FTC), the Equal Employment Opportunity Corporation (EEOC), and the Consumer Financial Protection Bureau (CFPB). These are some of the agencies that are in charge of how we experience the workforce, financial systems, and various ways that we interact with these corporations who extract our data. So, seeing these agencies step up and say, "Hey, we actually have policies in place that are meant to protect human rights, and we're going to try to leverage some of that power in favor of those human rights," gives me a little bit of hope. The most

recent action against Rite Aid on facial recognition from the FTC is a solid example. It's not everything we need, but it's a lot more than most have done to ensure we are heard and our rights are preserved.

I'm looking to see more of that, not that I have this blind trust in government, but I'm looking to see more agencies step up and say, "We believe in human rights. This is a violation of human rights. We believe in civil rights. This is a violation of civil rights," and exercise the power that they have to protect us.

EB: What does successful privacy and cybersecurity preparation look like?

TP: I'll channel Una Lee now and the Consentful Tech Project. It's consent, right? They have been trying to push us toward a more consentful technological world for a long time. They authored the Building Consentful Tech zine and we also have the things we outlined in the Consentful Tech Curriculum, which I coauthored, with an understanding that consent is going to be one of the hardest things to systematize. It really takes a commitment to revocability and reversibility that I see a lot of resistance to when it comes to extracted data by companies. But I support Una and her team's struggle of trying to push us toward a more consentful digital society. The five principles in the Blueprint for an AI Bill of Rights can also be useful here:

- Safe and effective systems—you should be protected from unsafe and ineffective systems.
- Algorithmic discrimination protections—you should not face discrimination by an algorithm and systems should be used and designed in an equitable way.
- Data privacy—you should be protected from abusive data practices via built-in protections and you should have agency over how data about you is used.
- Notice an explanation—you should know that an automated system is being used and understand how and why it contributes to outcomes that impact you.
- Human alternatives, consideration, and fallback—you should be able to opt out where appropriate and have access to a person who can quickly consider and remedy problems you encounter.

If anyone who leverages data and digital systems, uses the internet, leverages any kind of digital tool, or has a tech company considers those principles, we will be much further along. And of course, I live by the Detroit Digital Justice Coalition's Digital Justice Principles, which were inspired by the environmental justice principles. Allied Media Projects also has network principles I have internalized. We all have these principles that help us guide the way that we engage with communities, neighborhoods, and systems. All government agencies and tech companies should consider at least the Blueprint's guiding principles when they're designing, developing, deploying, or purchasing these systems. A healthy cyber ecosystem would be one that prevents those harms by following those principles.

EB: Would you say that your work is or could be to support us, I'm using us in the general sense, to establish these principles of what is consentful?

TP: It's definitely part of my mission. As of late, my work has felt like it's more of trying to shift narratives and politicize folks regarding what's out there that can be leveraged to push for more responsive legislation or more responsive policy on a local level and federal level. I've served as a

community educator in that regard and have done consultation with policymakers, etc. I look forward to supporting a future that implements some of these consentful systems by following the leadership and guidance of Una Lee and the Consentful Tech project, because I do see that as a passion. Truly consentful systems are going to be one of our most difficult challenges, because agencies don't want to give you back that data. It's worth lots of money.

EB: Considering what you just said, what support do you think you would need to work successfully at scale?

TP: I would like for policy and decision-makers to move beyond partisanship and recognize that these systems impact all of us. There is no blue, red AI harm. We all leverage the internet. Our families have access to the internet, our elders, our young people, all of us. And even when we don't have access to the internet, these systems still have access to us. We should all be collectively creating systems that are not harmful. That should move us beyond political lines. I need for policymakers to move. I need them to think more at a human level and less at a polarized political level. And I know the personal is political, but I need them to take these principles very seriously. I need them to push for it to be legislative policy within the agencies. I need them to hold the civil rights agencies and departments within all of these governmental agencies accountable, and I need folks to not be elected or reelected, if they don't take this seriously. How we currently navigate society online and offline, as well as how we experience our digital and literal futures are at stake.

EB: I hear that answer. Let's say that I'm a policymaker again, and I'm meeting with you one-on-one. I want to make a task force and put you at the head of it, or not even make a task force, but I see the work you are doing already and I want to support that. What would you need from me specifically?

TP: See, that's what's complicated. There are so many task forces that exist for these things. It's difficult for me to say anything beyond I need them to act on the millions of recommendations that they have already received. I need to see legislation actually move and not get stuck because of partisan politics. I need a legislator who is an advocate who purely listens to community voices and then takes those voices and makes policy that will pass. They need to be somebody who's willing to have nonpartisan or bipartisan cooperation to push through policies that are rooted in these principles that need to become actual local, state, and federal legislation. Now, beyond that, I don't think a policymaker can help me as an individual outside of passing a policy and pushing against pervasive, deceptive narratives.

EB: Maybe policymaker is not the word I should be using. But with the investment that's coming down the pipeline that is already actually lead, certain branches or bullet points like the Digital Equity Act necessitate some of the funding be spent on keeping the internet equitable. Do you think, as a government official, it would be possible for me to support you in accessing that funding?

TP: Yes, that's actually a conversation we've been having at Detroit Digital Justice Coalition. Like what's happening with this $1.5 billion that's supposed to be making its way through these communities? How can local grassroots organizations that have been committed to this work be seeded with the resources to do on-the-ground engagement; have real community trainings on how to be consentful and how to secure

your data; have real community trainings on how you engage with the political system; how you make a public comment. How do you pursue legislation? How do you ensure that legislation that you're pursuing makes it to be passed? I definitely think that that money should be leveraged to see those organizations who are committed to doing that work, but don't have the funds to do it. We need a grassroots level groundswell that is more effective than all the lobbying that tech companies have been able to do at a legislative level.

This interview has been edited for length and clarity.