THE DECENTRALIZED WEB OF HATE

WHITE SUPREMACISTS ARE STARTING TO USE PEER-TO-PEER TECHNOLOGY.

ARE WE PREPARED?

A REPORT BY:
EMMI BEVENSEE
&
REBELLIOUS DATA LLC

SEPTEMBER-2020

THE BEGINNING

I'm in a community called Scuttlebutt which uses Peer-to-Peer technology. This is a type of technology that works radically differently from the internet as we know it now and offers a powerful vision for a resilient and sustainable future for technology and social movements. One evening, a friend who is a developer on Scuttlebutt and also has marginalized identities like myself messaged me and a small group of others with great concern writing:

> "Ok - so we have nazis already using scuttlebutt. When the NZ shootings happened I had a dream that in the news it was announced that they had been using an enclave of scuttlebutt to organise and radicalise. It seems inevitable that this will happen…"

It continued a long conversation about the risks created by these radical technologies. My friend was genuinely afraid. So was I. And I still am. Like so many others, he had put a ton of work into cultivating both the community and the technology. He was scared both that the product of so many people's love would become a central aid in white-supremacist organizing and that the community wasn't ready to deal with the fall out of such a "nightmarish vision."

In most Peer-to-Peer communities it is impossible to surveill them or know how many people are using them because they are secure and often private by design. The only way to even catch a glimpse of how many white supremacists are using them is when they post on leaked forums or public websites. Otherwise, unless their conversations are infiltrated, we can only see the tips of the iceberg of the violence (or good!) facilitated by these technologies. We can see the initial post encouraging people to switch to the P2P encrypted messaging service but we can't know how many did unless anti-fascists infiltrate and expose it. We can see when people admit to posting a white-supremacist shooter's manifestos to resilient file hosting services but it's hard to find them and we can't remove them everywhere even if we do. We can see posts showing people how to effectively fundraise and buy firearm 3d printing kits or bomb-making materials with cryptocurrencies, but we can't know how many people have; until it's too late.

Many in the communities have converged around the common purpose of seeding the positive futures offered by p2p technologies while trying to mitigate the risks that scared us. This paper attempts to cultivate that hope and be realistic about the risks in the spirit of emergency and optimism for the future of the decentralized web.

Executive Summary

White supremacists have begun to seek more alternative online services, including Peer-to-Peer technology (P2P), as increasing pressure is applied to mitigate the rapid growth of white supremacists organizing through the Internet on more traditional centralized forms of internet and electronic service providers. In this report I define P2P systems for a non-industry audience, explain how and why white supremacists are using them, and show how we can utilize the strengths of P2P systems for positive social impact. The primary P2P systems used by white supremacists are: file storage, forums, communication, and funding. The primary threats of using P2P technology to spread hate are the organizing of hate-based violence, organized or dispersed harassment, and the facilitation of the spread of harmful or illegal hate content. Many in the P2P community are taking steps to reduce the potential abuse. P2P technology offers incredible potential for human collaboration but also poses some inherent challenges. This piece asks the critical question: how can we navigate the uncharted terrain of P2P technology without surrendering its potential benefits or minimizing the risks inherent to it?
Keywords: social media, P2P, hate, fascism, coordination, white supremacy, decentralization

Key Points

Radicalization is becoming harder to address. Major platforms like YouTube use imperfect algorithms for both recommendations and automatic content moderation. They host communities that can misinform and radicalize impressionable users. “Radicalization” refers to pipelines where users are exposed to more extreme forms of racist ideologies and behaviors over time. Centralized approaches to moderation, such as a top-down moderation or safety team, don’t work on P2P technology because the technology itself relies on decentralizing authority. As more white supremacists continue to migrate to P2P technology, the risk that they organize violence through these tools also increases.

Modern hate is not as responsive to top-down deterrence. As many white supremacists themselves expand use of “leaderless” tactics, they are becoming more agile at routing around centralized approaches to thwart their efforts such as policy, automatic content moderation, or the arrests of “lone-wolf” attackers. The decentralization of white supremacist groups is being increasingly facilitated by irrepressible and encrypted P2P technology. As such, many methods from typical government systems and structures, such as legislation or surveillance, are proving less effective at the more modern threat landscape. Only a network can defeat a network.

There are emerging decentralized solutions. Certain P2P tools have introduced novel ideas for combating harmful content. Some platforms have unveiled user agreements and urged their communities to block support for problematic tools. Other platforms have introduced “abuse audits” to identify and mitigate potential threats to users. Because of the technical and social nature of the problems we face, our solutions must also be largely decentralized.

Decentralization helps to solve many problems, but also raises new challenges. P2P technologies can advance many of society’s greatest coordination problems, from public transportation and supply chains to positive social connectedness and collaboration. However, the challenges that they ask us to face don’t have easy solutions.

Table of Contents

Introduction

The dot-com boom of the early nineties saw a rapid and exponential explosion in the types of content being shared. The social web epitomized by social media, which we refer to as the web 2.0, saw a similar rapid expansion of use about a decade later. In both cases, the proliferation of harmful and even illegal content caught designers largely off-guard. This is partly due to the lack of foresight in the form of network and content governance standards that could prevent its exploitation to facilitate hateful and extremist movements. The use of crowdfunding by white supremacists to raise capital for supremacist activity highlights the challenges posed by the social infrastructure of the web 2.0 that we continue to contend with today.

We are now headed into a new era of the Internet — the web 3.0— which uses more decentralized and less easily controlled technology. While white supremacists already fundraise with crypto-currencies, technological affordances like irrepressible Peer-to-Peer (P2P) file storage and encrypted communication are just starting to be used to organize and propagandize attacks. Notably, existing policy proposals attempting to address illegal hate content online will have little to no power in addressing the same content on the P2P Internet. Various organizing attempts of white supremacist attacks have already utilized P2P technology to facilitate white supremacist violence. However, the insights we gain and measures we recommend in this early phase of the decentralized Internet will determine the extent to which we will be able to mitigate future white-supremacist attacks using the P2P internet.

Through this report, the hope is to get ahead of the hate curve of web 3.0 and shed light on these issues while recognizing and capitalizing on the incredible value offered by the tools themselves.

The Centralized Internet

It's important to understand the nearly ubiquitous centralized nature of most online technology to understand the rise and appeal of decentralized P2P networks. In simplified terms, the way the Internet currently works is that your computer sends a request for information to a larger computer called a server, which is hosting the information of one or more websites. That server sends you back the website and whatever information you requested. The server stores all the information of that site in one place (more or less), which makes it easier for them to remove content and verify users. However, this centralization of technology also centralizes power.

What is P2P?

Understanding P2P technology first requires an understanding of *decentralization*. To decentralize a piece of technology is to fundamentally change the way it works by distributing authority rather than privileging one part of the system (such as the centralized servers from above). Decentralization means taking the parts of a system and spreading out the responsibility, trust, and power across the whole system, instead of concentrating them all in one part. Generally decentralization avoids single points of failure, such as a server, so that even if one center of power is attacked the whole system remains uncompromised. This spreads responsibility for the network to more parts in a more horizontal manner. To illustrate this concept in a more accessible manner, we can use governance parallels - a dictatorship is reminiscent of hyper-centralization, while a more horizontal and democratic system of local governance councils resembles decentralization.

Decentralization of technology, like other software, generally relies on *protocols* that allow the systems to work. A protocol is a set of standards that allow computers to run software or communicate with each other. Since a protocol, in this case, is just a language for communication, anything can be built to pass between computers in that language. Email is an example of a protocol. A decentralized protocol is a language for a decentralized technology to perform some action such as pass information. A *client* is some type of user interface that allows a user to utilize a protocol. Protonmail and Gmail are examples of clients that utilize the protocol of email.

The relevance of decentralization, protocols, and clients to P2P technology will make more sense by looking at what P2P technology actually is. The website Tech Terms defines P2P by saying:

> *In a P2P network, the "peers" are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as a client.*

To access Facebook your computer asks Facebook for the data on some page and they send it back to you from a centralized server. On the P2P Internet you are able to both host and share content directly with other computers.There are a wide range of technologies built in this way, ranging from P2P forums to blockchain cryptocurrencies. The P2P developer and user communities encompass many different movements and belief systems, from models of P2P economics to the communities more focused on the decentralized web, often referred to as the dweb(pronounced Dee-web). Dweb adherents range from free-speech fundamentalists to low-overhead, resilient communities using P2P Internet with common devices through a shared protocol known as a “mesh-nets.” There are tensions not just at the level of beliefs, but also code, between freedom of speech and dweb adherents invested in removing harmful or illegal content.

Generally speaking P2P and decentralized technologies tend also to be open-source. According to dictionary.com open-source is, “pertaining to or denoting software whose source code is available free of charge to the public to use, copy, modify, sublicense, or distribute.”

The most well-known example of decentralized, P2P, and open-source technology can be found in *blockchain* and *crypto-currency* technology. A blockchain is fundamentally a digital ledger keeping track of who has sendt what to whom. The ledger is decentralized in the sense that any public or private computer can store the transaction record of the currency, and can participate in the process of mathematically proving the transactions to be accurate, which are also available publicly. Crypto currencies are unique to and reliant on decentralized technology because they are premised on a public trust that is evident in the same transactions and mathematical proofs being stored on several computers at the same time and available to review by anyone anywhere. Crypto currencies are most often forms of digital money on a blockchain. Not all blockchain projects are about currencies but it is the most common form. So the protocol for a given crypto currency is the way that it works itself, whereas the client would be a wallet that allows you to exchange that currency.

P2P and decentralized technology are so popular that even a mainstream social media platform like Twitter is investing in a project called BlueSky to develop decentralized and open-source social media standards. Despite utilizing centralized infrastructure Twitter, Facebook, and the like have largely been unable to completely stem the tide of hate and disinformation content and appear to see decentralization as a possible solution. With all of this popularity, it is no surprise then that bad actors are taking notice as well.

Centralization or Decentralization?

The P2P domain exposes tensions in opposed rights. Decentralized networks have a unique configuration that relies on multiple computers/servers to remain operational. So it’s generally technologically impossible for a central authority, whether that be a forum moderator, a platform policy enforcement team, a domain host, or law enforcement, to dictate speech and conduct of users. Sarah Jamie Lewis of Field Notes in Resistant Tech writes, “decentralization is the degree to which an entity within the system can resist coercion and still function as part of the system.” Definitions like these show how the political dimensions of P2P and decentralization are interwoven with technical specifications. In comparison, centralized networks don’t have such limits because of the centralization of their infrastructure, control and protocols.

From a technical perspective, one could argue that complete freedom of speech would require no centralized authority that can remove or moderate content. However, the ability to remove dangerous or illegal content arguably creates a space that is more open and inclusive for marginalized individuals who may feel that their speech is chilled by interfacing with hateful threats. Therefore, moderation could also be considered paramount to living in a world free of hate-based violence and promoting more speech.

P2P technologies can protect the rights of marginalized people to organize for their human rights, but that same technology makes it possible for white supremacists to leverage privacy and censor-less systems to promote their bigoted and racist ideals. The same technology that makes P2P technology resilient against censors, also makes it resilient against things like natural disasters and poor Internet connectivity. In countries where the government represses information sharing or access to the Internet is blocked, P2P technologies can help people get connected.

Centralization, such as a server controlled by a corporation, allows us to quickly remove dangerous content but it puts the control for what constitutes “dangerous” in the hands of a privileged few.

Radical democratization of the responsibility for maintaining a healthy Internet that respects difficult discourse, free speech, and the rights of marginalized persons to safety online is the great task of the P2P era.

As decentralized technologies mature, they will likely occupy larger and larger portions of our day-to-day use of the Internet. As such, the tensions posed by choices in technological architecture — how we build a website or software — reflect tensions in different freedoms.

Why are white supremacists migrating to P2P technology?

Modern white supremacist movements have international funding and material support stream from individuals, states, and corporations. They also have similar top-down support from prominent figureheads and outlets. Parallel to this support, these movements show a grassroots system of leaderless self-organization and funding streams. This bottom-up ability to move in swarms and small groups is akin to the Leaderless Resistance ideals many 80’s and 90’s neo-nazi gangs co-opted after witnessing their efficacy in leftist movements. This leaderless movement is now further empowered by the Internet.

This leaderless and more horizontal movement structure is perfectly suited to P2P technology, making decentralized tools more appealing to many white supremacists and individuals. It’s often hard for white supremacists to network or build trust because they are under constant surveillance by activists and law enforcement and the vast majority of people are opposed to their views. As such, privacy and the ability to build trust without exposing themselves makes

P2P technology useful. Many white supremacists facing a litany of legal and social ramifications such as arrests and losing their jobs. This places the entire responsibility for maintaining an organization in the hands of a select few creates a very high-risk structure because if they go down, they take the organization down with them. Since P2P systems are generally not overly centralized around individual users, it makes their structure more resilient for both activists and white supremacists seeking to avoid these single points of failure.

Decentralized and open source technologies play an important role in keeping the Internet healthy. But like any technology, they can also be harnessed by bad actors — and employed to make the Internet a less healthy, more dangerous place.

Some examples of how groups in the U.S. are using P2P technologies to spread disinformation, amplify toxic content, and incite violence will be highlighted in the next section. As popular online platforms like Twitter and YouTube have begun to crack down on white supremacists following the activism and reporting of civil rights organizations(1, 2) these online communities don't just go away. Instead, there's been an exodus to spaces that are more difficult to scrutinize and moderate, but still have the potential to reach a mass audience. Successful efforts to thwart online white supremacist terrorism have done things like driving the neo-nazi organization American Identity Movement, formerly known as "Identity Evropa," into less action and recruitment through a series of exposés and leaks of private conversations, getting white supremacists removed from payment platforms, pushing back on media and advertisers profiting from white supremacy, and interrupting service to 8chan. However, with this shift, these white supremacists are increasingly migrating towards more censorship-proof and private methods of decentralized collaboration such as P2P technologies. Meanwhile there has been disagreement about this in the P2P communities as some leaders themselves begin to adopt "anti-social justice warrior" ideology despite critiques and calls for dialogue from others in the movement.

P2P tech can help us build a better world but it's difficult.

Peer-to-Peer systems simultaneously hold the keys to solving a wide array of coordination problems and unleashing harmful web content to spread unabated. There is a lot that white supremacists are already doing with these protocols, but there are also many creative efforts to minimize that harm without surrendering the radical potential of these systems. Because the future of hate movements is increasingly looking like it will be decentralized, anti-hate tactics must also adapt to this rapidly shifting terrain.

For this project, I interviewed 6 experts, held 4 workshops, attended 3 additional workshops on the topic, had countless informal conversations with various actors in this field, and held a community-wide open editing process. Concurrently I was also working myself on these issues in the P2P and anti-hate space as a Mozilla Open Web Fellow and a Doctoral Fellow at the Centre for Analysis of the Radical Right. Additionally I run an open source social media analysis platform called SMAT and a social good data science consultancy called Rebellious Data LLC. This is an exploratory study utilizing qualitative and embedded ethnographic research methods as quantitative methods are largely obstructed by the nature of the technologies.

Use of P2P tech by white supremacists

There are three key areas in which white supremacists are already using and developing P2P technologies however each of these risk areas is balanced by their potential positive uses.

File storage

Tools such as Inter-Planetary File System and Bitchute are being used to host hate content in ways that are extremely difficult to censor. The Internet Archive is working to make a P2P version of its archives, which also hosts hate group content. While the prospect of resilient hosting of things like manifestos and terrorism guidebooks may be frightening, tools like IPFS and a P2P version of Internet Archive also have valid use cases such as preserving evidence of war crimes, activism, and citizen journalism amidst pressure from repressive governments.

Rob Monster, who makes a living protecting alt-right websites such as Gab through his company Epik, uploaded the Christchurch attackers manifesto to IPFS. Similarly, Weev of Daily Stormer infamy said that he would now be posting all of his written and video content on IPFS after GoDaddy, Google, and Cloudflare refused to support his neo-nazi pet projects. BitChute was publicly scolded for its hosting of a wide range of white-supremacist vloggers.

Forums

There is a wide range of forums and social media that employ P2P technology. The potential of P2P social media is profound, such as for emergency resilient communication infrastructure in areas with low Internet penetration. However, any tool used for connection, especially ones that are more private and secure, will be abused by white supremacists and other bad actors. In this case, many white supremacists are using, have attempted to use, or are developing P2P social media systems.

After multiple terrorists were radicalized on 8chan and then used it to promote and gamify white-terror mass shootings, and after a sustained campaign against it by activists including 8chans original creator, they were finally dropped by various providers and hauled before congress. As their service was dropped, a clone began to be advertised which was on a distributed service called Zeronet. The advantage of Zeronet is that it could not be censored or taken down if a DDoS protection service or server decided that 8chan was a liability and dropped them. Ron Watkins, the web manager of the white supremacist-friendly platform 8chan, claimed not to know anything about this clone, though he had created his own proof-of-concept P2P forum. These types of mutations like ZeroNet don't require a central authority in the same way that they don't respond to things like subpoenas. Though they have not released all of the data yet, Ron Watkins -- in cooperation with "LimTheNick", Vanwa Tech, and Is It Wet Yet -- are working on something called "Project Odin" which claims to be a P2P Content Delivery Network that could help protect 8chan and its descendent 8kun from constant deplatforming by letting users help host the website's data on their computers.

Communication Channels

Additionally, many white supremacist terror networks have turned to decentralized communication technologies such as Riot built on Matrix (which have been rebranded as Element and Element Matrix Services, respectively) for encrypted direct messaging capacity. While this technology also provides critical infrastructure for human-rights activists across the globe, it is also used by white supremacists like the Feuerkrieg Division who aspire to armed white-supremacist insurrection using explosives and illegal firearms and targeting major infrastructure such as electrical grids. This organization is modeled in part after their sibling organization The Base, who are scrambling after a series of arrests and high profile exposés following various related murders, bomb plots, and attempted murders. Their efforts include an attempt to start a large-scale protracted race war narrowly thwarted by antifascists and the FBI and they organize, as well, in part over Riot.

Funding

White supremacists and forums connected to murders are using privacy-focused cryptocurrencies to fundraise without revealing their identities to authorities or even each other. The anonymity of cryptocurrency isn't fundamentally different from that of cash, and a right to anti-surveillance spending does exist. However, users fundraising neo-nazi terror organizations without any knowledge of each other does raise difficult questions.

After the white nationalist gathering in Charlottesville where Heather Heyer was murdered, an anonymous donor gave infamous white supremacist and Daily Stormer founder Andrew Anglin 14.88 bitcoins. This amount is an allusion to the white supremacist 14 words and 88 stands for 'Heil Hitler'. At the height of bitcoin, this would have been nearly $300,000. Another of Anglin's wallets for Daily stormer shows that he sent and received 10 Bitcoins in over 1300 transactions. Relatedly, many white supremacists link to their page on the social network Minds which offers built-in decentralized micro-payments. This all shows both the ability to fundraise through small payments and spend the money to unknown ends. This isn't a particularly uncommon occurrence though. Most fascist websites now contain the ability to donate in various cryptocurrencies such as Bitcoin or Ethereum, but also inherently more anonymous currencies such as Monero. The Twitter account @NeonaziWallets tracks the wallet balance of known accounts, but most of this is happening beneath our awareness.

What can be done?

Hate in the P2P domain is a huge threat but addressing it requires stretching our practices, minds, and code in novel ways.

Some of the key top-level threats of hate-groups in the P2P space are:

- Organizing hate-based violence
- Organized or dispersed harassment
- Facilitating the spread of harmful or illegal content related to hate

Ethics in the P2P space

There is a version of Conway's Law which suggests that the tools we develop reflect our own values and communication styles in the organizations where we work. In coding, an "affordance" is how software is used regardless of how it's intended to be used. Our tolerance for certain affordances at the code level is a reflection of our values going into the process. The diversity of different ethical and political values, as well as ideological motivations, in the P2P space impact the types of tools that are developed and how they are implemented. What is built and how, is impacted by whether its designers think the potential good of a tool is outweighed by its potential risks such as use by white supremacists.

For many in the P2P space, particularly those influenced by political ideologies such as techno-libertarianism, a belief in a combination of maximized liberty through free-markets and technology, the affordance of malicious use of their tools is understood as a necessary risk to advancing goals like freedom of speech and curtailing state overreach. To those in the P2P space more influenced by leftist and social justice ideologies, affordances such as use by white supremacists using a technology is something to be counter-acted as much as possible while still trying to leverage the potential of the tool. Further, there is a subpopulation of people in the P2P development space who themselves identify with white supremacist ideologies though they may take the cover of other political ideologies or dogwhistles.

There are also those in the P2P space who are driven not so much by political or moral ideology but as by curiosity of the technical and mathematical possibilities. For this group, topics such as zero-knowledge proofs - a mathematical and technical system that can prove a transaction occurred without revealing information about either party-- are interesting in and of themselves for their roles in things like cryptography and secure transactions. This group is less concerned overall about whether any given group, hate or otherwise, uses their tools and more that they can advance the technology and theory.

Depending on one's values heading into building or utilizing P2P technology, the tool can represent very different possibilities. A developer for a P2P project called Secure Scuttlebutt mentioned an instance of this tension in the community when he discussed, "Whether the lowest levels of code and protocols should be impacted by human concerns or whether they should be 'neutral'." He, like many others more concerned with the social implications and contexts of these technologies, tends to view technology as inherently political for the ways it interacts with and is formed by the biases of politics in general. Those more guided by purely technical concerns or techno-libertarian ideals in the crypto-currency space tend to emphasize the importance of "neutrality" at the level of code as a form of P2P purity. Whether one thinks code can be neutral or not influences the affordances considered acceptable in the technology developed.

Those guided more by right-wing ideologies in the P2P space tend to focus more on things like crypto-currencies and extremely privacy focused free-speech tools, which are more likely to be abused by hate-groups whether that is the intention of the developers or not. There are powerful positive implications in both P2P privacy tools and crypto-currencies, however it is important to acknowledge this potential alongside their built-in affordances.

Those focused more on social-justice influenced liberatory tech tend to focus more on P2P tech geared towards connecting people and try to build in more protections to protect abuse. Because of the emphasis on "neutrality" in much of the blockchain space, there tend to be more liberal or social justice-minded people gravitating to the not-strictly blockchain-based projects such as SSB, The Hypercore (formerly Dat) Protocol, or Holochain. These systems are fundamentally different from blockchain projects because they rely on the power of networks of human users to define what the protocol does rather than entrusting the math itself alone.

The reality of these communities though is that many ideologies and motivations overlap and most people that I've spoken to have nuanced and complicated views on a range of these issues. Tensions at the level of code are embedded in the social context that creates them. The freedom of speech represented by an uncensorable P2P protocol interacts with the freedom to not experience racist violence organized through the very same protocol. Therefore it is important to investigate how some actors are pushing back against hate in a technological space that is, by design, difficult to censor.

The curious case of SSB

Secure-Scuttlebutt (SSB) is a P2P protocol that helps devices communicate but doesn't tell them what to talk about. This means that you can build everything from a forum to a chess-app on top of it. Much of the seed community of the SSB network is influenced by solarpunk and "walkaway" ideologies about sustainable and equitable technology. Many in the community report hope for the ways that SSB can help aid with things like rural connectivity in the Amazon jungle, helping with coordination amidst natural disasters, and providing autonomous control of communication infrastructure to otherwise marginalized communities. However, according to my interviews, there are already many problems such as some neo-nazi users despite efforts against them. A lot of core developers I spoke with are also concerned that if the platform became widely used, as some hope it will, it would bring in a flood of those attempting to organize terror or harassment campaigns. To mitigate this they have attempted a range of different strategies:

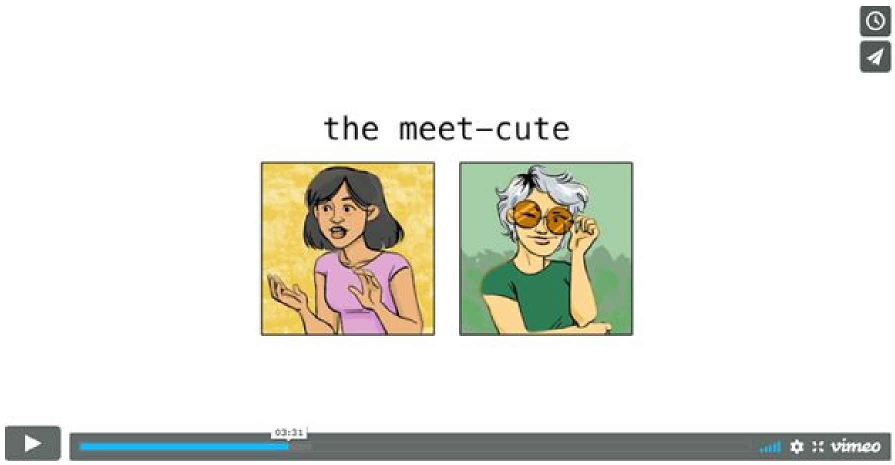
Diversifying conversations Many of the core developers recognize the need for political and social insights in the process of development. As such they have supported efforts to bring in more diverse pools of users and voices into conversations about what gets built and how.

Community as Immunity Because of the way SSB works, moderation and what gets amplified is decided by trust and how connected someone is in the network, rather than by an algorithm optimized for engagement like on Twitter or Youtube. In order for a message to spread in the network, that user must be trusted. According to the developer André Staltz, this makes it less attractive to those trying to amplify things like hate or disinformation. Furthermore, when you block someone, in addition to refusing to propagate their messages, the block is public so it sends a signal that this individual is untrustworthy in some respects. In this sense, SSB relies to some extent on reputation networks in order to isolate malicious users.

Abuse Audit The #abuse-audit channel and accompanying processes were an attempt to map out possible vectors for abuse in the network. Using the collective results of this process, mitigation strategies were developed for a range of scenarios.

The Planetary approach Planetary is an iOS client built using the SSB protocol and is geared towards mass adoption. Planetary has made use of somewhat controversial Venture Capital in a good faith effort to build a widely accessible client that also addresses some of the dangers of P2P technology through decisions at the level of how the code works. Some worry that the use of Venture Capital by Planetary will provide incentive towards dangerous mass adoption while others argue it will provide the funding necessary to create healthy mitigation and compliance structures.

Aesthetic choices and signalling SSB has never advertised itself as a free-speech platform though it does have many of those qualities at a technical level. Additionally designers have purported that they pursue a range of aesthetic choices aimed at attracting or repelling certain types of users. For instance, clients and the official webpage often use pastel colors, on the homepage there is a cartoon about an inter-racial queer love story that explains how scuttlebutt works, and many clients have implemented content warnings. Interviews stated this was all intentional to turn-away hateful users.



Gab versus Mastodon

Gab is touted as a “free-speech platform” but quickly became a white-supremacist echo-chamber. When Gab started getting shuttered by various service providers including the Apple and Google app stores, they decided to switch their structure over to becoming an instance of Mastodon, which is a more decentralized form of server federation. A server federation means that you can build your own server and community in the way you want and still allow it to communicate with other servers through the Mastodon protocol. When Gab attempted this switch to Mastodon they encountered a lot of forms of resistance from much of the Mastodon community (some forms more effective than others). Mastodon’s core development team put out a statement saying:

> *“Mastodon is completely opposed to Gab’s project and philosophy, which seeks to monetize and platform racist content while hiding behind the banner of free speech. Mastodon remains committed to standing up against hate speech; for example, our new server covenant means we only list servers on joinmastodon.org that are committed to active moderation against racism, sexism and transphobia. The Mastodon community does not approve of their attempt to hijack our infrastructure and has already taken steps to isolate Gab and keep hate speech off the fediverse.”*

They encouraged all Mastodon instances to block federation with Gab and hard coded blocks of Gab into many of the apps. This has worked to some extent. While Gab is still live, it is largely isolated. While it is largely impossible to block misuse at the points of decentralization, many organizations have pursued deterrents at the points of centralization such as their normal websites, clients, and main portals.

The trials of Ethereum

Ethereum is a "global, open-source platform for decentralized applications." It is a blockchain and a crypto-currency protocol through which you can build all kinds of currencies, applications, and even Decentralized-Autonomous Organizations (DAO). One of the founders of Ethereum, Vinay Gupta spoke publicly against white-nationalism and the alt-right in the P2P space encouraging that people should give "not one cent" to them or otherwise support their projects. He was subsequently attacked by the neo-nazi blogger, Andrew Anglin. In response, Gupta tweeted:

> *"You should fork off. We will not be good hosts…. We will collude against you. We will make your lives miserable. We will… figure out underhanded-yet-ethical ways to make your project fail… By all means put your entire life's work into the hands of people who hate you… We do infrastructure. You depend on us."*

To some extent, Gupta's statement is an ambitious bluff because there's only so much Ethereum can do to stop neo-nazis from using their technology. Websites like Fascist Forge have Ethereum donation buttons and many in the cryptocurrency community took the side of the Daily Stormer in this debate. However, it's critical that one of the most prominent blockchain projects took a vehement and public stand against white-supremacists when many others just shrug and ignore the problem.

TrustNet

TrustNet is a new and exciting system developed by Alexander Cobleigh that is designed to be a Peer-2-Peer formalization of subjective moderation through networks of trust. The system was proposed in his recently published Master's thesis, which also describes *subjective moderation*. Subjective moderation here is the concept that each chat participant can subjectively designate who they trust to moderate content on their behalf, thus delegating the power to hide abuse and block trolls.

He describes TrustNet as: a system for interacting with and managing trust. Underlying the system is a transitive trust algorithm. The system as a whole was originally intended for use in combination with peer-to-peer distributed chat systems, where peers assign trust (a value between 0.0 and 1.0; 1.0 being complete trust, 0.0 the complete absence of trust) to other peers.

He advocates for assigning trust through human-meaningful labels, such as using the label *friend* to represent the trust value 0.75. TrustNet uses the Appleseed algorithm to walk the trust graph, using transitive trust, in order to compute a subjective ranking of the most trusted participants as seen from a particular participant. This ranking is then refined using a clustering technique, resulting in a group of the most trusted peers.

The result of all this is that the system can be used to do things like suggest new friends or even moderate questionable content. Because TrustNet works transitively through peers, it can also be said to help propagate trust through a network. This process works similarly to how technologies like Scuttlebutt already work and therefore works well with similarly designed P2P chat systems.

The question of scale

The many attempts and difficulties of those working for social justice through P2P technology give us a glimpse of how we can utilize these tools to build a better world and what might be standing in the way. But P2P is also about bringing technology closer to human behavior which asks us to answer more fundamental questions about what we want out of social networking, what is possible, and most importantly, how it interacts with the real world.

Community governance structures are a quintessential part of any commons management approach and this applies equally to the internet. This is why some P2P developers such as Darius Kazemi encourage people to build small, rather than at the scale encouraged by Silicon Valley. Robert Caplan of Data & Society emphasizes three different approaches to moderation:

- Artisanal: A small team of usually in-house moderators
- Community reliant: Models like Mastodon, Wikipedia, or Reddit that allow the communities to self-monitor for harmful content with trusted local authorities
- Industrial: This usually involves both machine-learning and the outsourcing of harmful content viewing to marginalized persons.

Other related approaches are local filters such "glasses moderation" in which a user decides what types of content they would like to personally filter. Non-P2P examples of this includes the Opt-Out misogyny filtering browser add-on. Relatedly there are phenomena like shared-blocklists which present their own difficulties and opportunities.

At each new level of scale, a community must utilize increasingly difficult and politically complicated general measures of acceptability and methods of enforcement. This is why much of how P2P harm reduction actually relies on more human solutions to technical problems rather than "silver-bullet" machine learning or the like that come with many pitfalls.

Social solutions to social problems

P2P technology, like society as a whole, has fundamental tensions between the trust we give a centralized body— Authority Mode — and the trust we give each other, which could be called

Freedom Mode. Authority Mode is in some ways easier and more convenient because an individual need not think as much about ensuring their own well-being and that of their community. However, as shown by the major social-media platforms, even total centralization is not a guarantee of the ability to perform effective content moderation at scale. Freedom Mode is much harder because it asks us to take responsibility for our environment, but it can be more democratic and more ultimately liberatory. P2P technology is introducing much more meaningful avenues of choice and as such uniquely frames this relationship between freedom and responsibility. So when hate begins to crop up on a technology that could give all of us more freedom, how do we react? These issues unfurl concurrently at the levels of both individual and policy level choices.

Legislation has extremely limited ability to repress the proliferation of decentralized technology, as seen with the failure of anti-torrenting laws designed to curb online piracy. As with 3d printed weapons, anyone can post the code anywhere and then anyone can download it. It's impossible to completely repress this technology short of eliminating the entire Internet or further centralizing it beyond even what is envisioned by China or Russia. The limits of technical and legislative solutions imply the necessary overlapping of multi-pronged approaches to mitigating hate-based violence more broadly. As such, we must work to align P2P technologies with prosocial values as much as is possible and prepare in the meantime for unintended negative consequences.

The deep and pervasive roots of racism and structural violence against minorities influence the contour and likely paths of any new technology. As things like structural racism and white supremacy already exist in the world, P2P technologies can either accelerate pro-social anti-racist coordination or hate itself depending on the ways we choose to engage with them at various levels. P2P systems mimic the questions of how we combat racism and intolerance in the real world. Since P2P technologies rely on the power of networks like physical human communities do, we can't just program hard rules into such technology. These human approaches to addressing technical problems are far more difficult, but they are also more sustainable in the long run.

The question of how we can build tools that aid existing social technology for maximized positive cooperation without unleashing dangerous consequences, such as augmented nazi-terrorism, is a critical question of our time. Rabble, from Planetary, discusses these issues when he says:

> "My hope is that we can build a social layer that lets us build a whole world where we don't need permission to participate or organize and create spaces that encourage egalitarian and humanitarian prosocial behavior. The web does a ton of that and even social media does a

> ton of that. And we have farther to go. If we’re successful [at using P2P technology for this] we will have new problems to deal with.”

The future of P2P technology is already upon us and the momentum is there for it to continue expanding and attaining more widespread adoption in the coming years. Therefore addressing these questions earnestly, openly, and early holds critical bearing on where the technology ultimately leads us.

The course of P2P overall depends largely on what type of communities flock to it and invest time and energy in these early days. Therefore, it’s essential that those invested in agency, multicultural thriving, and societal evolution lead the charge into this new domain. The P2P space opens wide this intimate and thorny nest of issues and asks us to grow collectively to face the next era of challenges. If we can steer it for good, a more complexly interconnected and meaningful future awaits us.

About the author:

Emmi Bevensee is a Mozilla Open Web Fellow, Founder of the Social Media Analysis Toolkit (SMAT) and Rebellious Data LLC. They are also a Doctoral Fellow at the Center for Analysis of the Radical Right. They received a MA in Conflict Transformation and Peacebuilding with an emphasis on decentralization of governance in conflict zones and studied Machine Learning in the iSchool PhD program at the University of Arizona.

Acknowledgements:

All of my successes are built collaboratively with the support of my partner. Special thanks to the Centre for Analysis of the Radical Right, Mozilla, Grant R. Vousden-Dishington, Ahmad Sultan, Dan Hassan, and countless others for supporting, believing in, and seeing the importance of my efforts in this and related domains. Thanks to all the interviewees, pre-readers, editors, and designers. Thanks to all of the hacktivists working to make this new interconnected world better for all of us. Without all of you this work would be impossible. ***You make believing in tomorrow easier.***

A REPORT BY:
EMMI BEVENSEE
&
REBELLIOUS DATA LLC

SEPTEMBER-2020