Digital Civil Societies: The Proverbial Double-Edged Sword

Even with its highly debated and controversial definitions, most scholars tend to agree on the purpose of civil societies: the advancement of an interest through the gathering and association of people beyond their immediate private life, outside of political state activities or interests. Heavily romanticized, civil societies have been framed as the pinnacle and epitome of democracy - both by existing and by their goals - due to their typical alignment with democratic values, as they rely on the freedom of speech and association to flourish, and make use of people joining towards a common cause. Just as much, they have been spoken of in either selective membership and secretive gathering places - such as women’s suffrage activists meeting in clandestine locations and freemasons - or very broad, public interactions with the intent of moving the masses - such as the yellow jacket protesters in France, or LGTBQ+ pride movements. Both cases, while polar opposites, lead to a vision that civil societies are incredibly special and/or unique. While true to some extent, this has the unintended consequence of limiting the perception of what is and what is not a civil society. Intention, goal, space and membership are some of the reasons why some or another group are not perceived as civil societies. Space, in particular, has shifted with the appearance of computers: physical spaces have been the only way to congregate for almost all of history, but with the invention of computers and the widespread use of the internet, digital spaces have been created. The internet has given way for a new ways of communication and interaction and by extent, associational life. Its biggest virtue - instant communication with anyone anywhere - is also its highest flaw: misinformation, polarization, antagonizing and the misuse of digital tools is rampant and growing everyday, with no signs of stopping anytime soon.

Digital spaces exist in so much as we interact with them. Where a physical space is guaranteed to be there even if there are no living beings in it, digital spaces have no proof of existence beyond their practical use expect for lines of code that make them up, living in someone’s computer, in which state they are not a space. What allows this space to exist is both highly technical and very accessible: engineers and scientists devise a technical way to make something accessible for casual users. Its growing list of contributors and participant is just as long as the diversity of opinions and views that, when put together, seem impossible to be able to coexist, and yet they do. Anonymous by design, the internet allows for people to connect without any attachment of themselves to the digital persona they present to others; while usernames and nicknames are common, complete anonymity is frequent enough to be the default. Having the same username across spaces does not guarantee they belong to the same user. Sometimes, one person can have multiple usernames, and everyone else would be none the wiser without some extensive investigation. This would sound like a very unlikely, if not impossible, scenario for anyone who has not been around the internet for long, which while impossible now, it makes a good case for analyzing the great difference the internet has made in the world.

Jorge Luis Borges, in his book *Fictions*, wrote a short story - Tlon, Uqbar, Orbis Tertius - about a very technical, absolute and unfathomable space, written in an academic style so as to throw off the reader: is this a real place (it could be, as the story references real-world encyclopedia and philosophers who have talked about the space) or is this just a tale the author is telling us (it can’t be real, as this is impossible)? As more part of our lives depend or heavily intersect with the digital world, it can be hard to look at the big picture and understand just how much of an oddity the internet is. The world this short story describes, in retrospective, might as well be the internet:

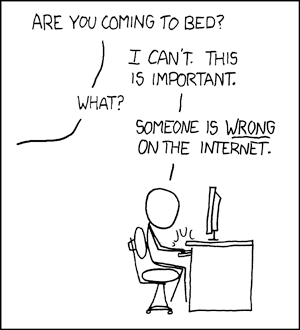
*It is conjectured that this brave new world is the work of a secret society of astronomers, biologists, engineers, metaphysicians, poets, chemists, algebraists, moralists, painters, geometers... directed by an obscure man of genius. Individuals mastering these diverse disciplines are abundant, but not so those capable of inventiveness and less so those capable of subordinating that inventiveness to a rigorous and systematic plan. This plan is so vast that each writer's contribution is infinitesimal. At first it was believed that Tlön was a mere chaos, and irresponsible license of the imagination; now it is known that is a cosmos and that the intimate laws which govern it have been formulated, at least provisionally. (Borges 1962, 5)*

Computers, networks, programs and applications are highly technical and done by scientists and engineers, and yet they are used (and destined for) non-technical people. It is this audience who determines what the platform is used for, and the engineers respond appropriately.

*In literary practices the idea of a single subject is also all-powerful. It is uncommon for books to be signed. The concept of plagiarism does not exist: it has been established that all works are the creation of one author, who is atemporal and anonymous. The critics often invent authors: they select two dissimilar works - the Tao Te Ching and the 1001 Nights, say - attribute them to the same writer and then determine most scrupulously the psychology of this interesting homme de lettres...*

*Their books are also different. Works of fiction contain a single plot, with all its imaginable permutations. Those of a philosophical nature invariably include both the thesis and the antithesis, the rigorous pro and con of a doctrine. A book which does not contain its counterbook is considered incomplete. (Borges 1962, 11)*

Anonymity is the default state in the internet. Social media and other platforms allow people to choose a fictional, arbitrary identity by which to present themselves to other people; in spaces where this is optional, or in plain connections, anyone saying anything might as well be the same person, as there is not much way to determine the authorship without some heavy tracking and surveillance. Someone, somewhere knows, but for the casual user, there is no way to tell the difference. This is sometimes used by knowledgeable parties who create multiple users or personas in order to give the impression to any third party that there is some interaction going on: it is not uncommon for people who seek fame to create an account, and then create thousands of other accounts to interact with this one they want to promote. In most cases these ‘fake’ accounts are created to promote something, but in others, they are used to sow discord and conflict by having one side insult, diminish or otherwise incriminate their target account, by which evidence they play victim and again get some sort of attention. From an outsider’s perspective, unless they have been following the situation carefully and/or dig deep into the details, it would be almost impossible to distinguish a real conflict from a staged one, as discussions and arguments (and the inevitable fight that ensues most of the times) are very common in social platform and are in fact one of the hallmarks of all communications and interactions in the internet.



Outside of artistic comparisons, it is this dual nature of the internet that makes it so hard to grasp and understand at the scale in which it really operates. This obfuscation is what led to the current monopolistic, monolithic companies that dominate the internet. Consider, for example, Google. What started as an indexing mechanism to search for keywords in pages, is now a conglomerate with all sorts of businesses in data collection activities. Pre-2013, where Snowden disclosed just how much information is actually gathered about civilians by the government with the help of these companies, most of the world did not give too much thought over the implications of the tools they use. A search engine just meant something to look up things, right? Unbeknownst to most, Google keeps a very detailed fingerprint about everyone that uses their products. Some cases are obvious: if you have a Gmail account - or any account in any of Google’s services - your information will be linked to it. Others get muddy: if you don’t have an account, your device, location and browsing pattern (among other information sources) can be used to give you a unique identity. Then all information is linked to this profile about you, even when you have not created it, nor consented to your information being collected, or to a profile about you being created. What ads you see, how long you spend on a page, what links you have interacted with, what did you deleted and its content, your searches, who you interact with, where you’ve been, what devices have been near you: things that we don’t normally think about or even know consciously are collected and analyzed routinely, and put together generate a very detailed picture of person’s life. A sufficiently motivated party can use this to incriminate someone by pretending to be them online (if they gain access to their accounts, which is potentially not too hard to do in most circumstances), and as digital records do not fall under the ‘reasonable expectation of privacy’ test, they are very easy to access by other companies, law enforcement and interested individuals without a warrant or any other legally binding reason or document.

Data mining for the purpose of targeted advertisement makes companies have very detailed information about people which, in the wrong hands, can lead to a wide variety of abuses. Sadly, reality has proven that the very existence of this model is harmful (as opposed to harmful only if used inadequately), as this massive data collection mas done mostly without users’ consent, serves corporate interests who most times don’t protect the data properly, and enable government surveillance. With their products and attractive gratuity, users don’t stop and consider the implications or hidden costs of the programs they use. Some scholars are critic of digital spaces being appropriate for civil societies for these exact reason: given their potential to serve as a vehicle for human rights violation, corporate interest and general misuse, it is counterproductive to consider the congregations inside these spaces to be free and for the advancement of something without external influence, when the platform itself limits freedom and uses ads and partnerships to influence their users. Because of this, many don’t consider digital spaces, and by consequence digital civil societies, to be legitimate carriers of change.

Despite the general ignorance, users are growing aware of the perils of corporate platforms - like Facebook, Twitter, Google - and are opting for privacy oriented, independent platforms, such as Mastodon, DuckDuckGo and Protonmail. Others rely on heavy encryption (which Protonmail makes use of, for instance) to keep their communication private to both the platform owners and any third parties that might be listening in somehow. Some have even started their own applications and forums to make sure that their information will be safe and that there will be no infiltrators in their members. If there are means to keep data secure - and by definition, the content of discussions, members, identities, and any personal identifiable information - and so avoid corporate interest and potential breaches to rights, then the criticism of appropriate use of digital spaces can be solved. While the question still stands on what will casual users do - encryption and non-standard platforms are not easy to come by and at times highly technical - privacy critics and data breaches make it easy for advocates to attempt hold these companies accountable and for casual users to educate themselves on the better ways to hold their sensitive discussions. An example of this is the website RiseUp, with an ’invite only’ membership to make sure it gets to their adequate audience; this website makes encryption for email and files readily available to its users, as well as offer a bitmask application and a VPN, both tools that ensure anonymity when browsing the web. This project is entirely volunteer run and is aimed at activists, radicals, journalists and any other party who deal with sensitive information and whose life could be potentially at stake if this information is found by the government. In several cases states have attempted to seize and search RiseUp’s servers to search for the offending data and have come up empty handed, as the heavy encryption makes the information completely unreadable and unrecoverable without the keys, who the account owners and no one else have access to. As such, digital spaces can be legitimate carries of change and can be exempt of external interest, albeit with the concession that this is the exception and not the norm.

Elaborating further on the topic of casual users, most people have some sort of social media profile, or make use of some or another platform where people contribute information. Similar to the advertising dilemma (in which companies collect information for them), recommendation algorithms play a heavy hand in most of the discussions around social media misuse. The way these algorithms work is, in theory, simple enough and allows for users to get the content they want; this is very similar to the argument for data collection, in which companies argue that they collect information to advertise the products to the proper audience. However, as shown by multiple studies and books, these algorithms are broken, frequently with their creator’s blessing:

“*The massive “library,” generated by users with little editorial oversight, is bound to have untrue nonsense. Instead, YouTube’s problem is that it allows the nonsense to flourish. And, in some cases, through its powerful artificial intelligence system, it even provides the fuel that lets it spread.(...) In recent years, scores of people inside**YouTube and Google, its owner, raised concerns about the mass of false, incendiary and toxic content that the world’s largest video site surfaced and spread. One employee wanted to flag troubling videos, which fell just short of the hate speech rules, and stop recommending them to viewers. Another wanted to track these videos in a spreadsheet to chart their popularity. A third, fretful of the spread of “alt-right” video bloggers, created an internal vertical that showed just how popular they were. Each time they got the same basic response: Don’t rock the boat.*” (Bloomberg, 2019)

“*The marketing of these universities is a far cry from the early promise of the Internet as a great equalizing and democratizing force. If it was true during the early dot-com days that “nobody knows you’re a dog,” it’s the exact opposite today. We are ranked, categorized, and scored in hundreds of models, on the basis of our revealed preferences and patterns. This establishes a powerful basis for legitimate ad campaigns, but it also fuels their predatory cousins: ads that pinpoint people in great need and sell them false or overpriced promises. They find inequality and feast on it. The result is that they perpetuate our existing social stratification, with all of its injustices. The greatest divide is between the winners in our system, like our venture capitalist, and the people his models prey upon.*

*Anywhere you find the combination of great need and ignorance, you’ll likely see predatory ads. If people are anxious about their sex lives, predatory advertisers will promise them Viagra or Cialis, or even penis extensions. If they are short of money, offers will pour in for high-interest payday loans. If their computer is acting sludgy, it might be a virus inserted by a predatory advertiser, who will then offer to fix it. And as we’ll see, the boom in for-profit colleges is fueled by predatory ads.*

*When it comes to WMDs, predatory ads practically define the genre. They zero in on the most desperate among us at enormous scale. In education, they promise what’s usually a false road to prosperity, while also calculating how to maximize the dollars they draw from each prospect. Their operations cause immense and nefarious feedback loops and leave their customers buried under mountains of debt. And the targets have little idea how they were scammed, because the campaigns are opaque. They just pop up on the computer, and later call on the phone. The victims rarely learn how they were chosen or how the recruiters came to know so much about them.*” (O’Neil, 2016)

These algorithms - who Cathy O’Neil calls ‘Weapons of Math Destruction’ - make heavy use of statistics and transmission models to get what they want to who wants it, and get what *they* want from who they want. In the case of Youtube, who is the subject of Bloomberg’s article, this is achieved by tagging videos with keywords, topics and authors, interlinked by graph models, which are then used to ‘recommend’ videos. Initially, the algorithm is innocuous: searching for music, it will recommend other genres of music. But as the spent time on the platform grows (more data on the user is collected, which is correlated with other topics for recommendation), the suggested topics get increasingly irrelevant and inflammatory, ranging from unrelated and not interesting to blatant misinformation and inappropriate:

“*YouTube’s inertia was illuminated again after a deadly measles outbreak drew public attention to vaccinations conspiracies on social media several weeks ago. New data from Moonshot CVE, a London-based firm that studies extremism, found that fewer than twenty YouTube channels that have spread these lies reached over 170 million viewers, many who were then recommended other videos laden with conspiracy theories.*

*The company’s lackluster response to explicit videos aimed at kids has drawn criticism from the tech industry itself. Patrick Copeland, a former Google director who left in 2016, recently posted a damning indictment of his old company on LinkedIn. While watching YouTube, Copeland’s daughter was recommended a clip that featured both a Snow White character drawn with exaggerated sexual features and a horse engaged in a sexual act. “Most companies would fire someone for watching this video at work,” he wrote. “Unbelievable!!” Copeland, who spent a decade at Google, decided to block the YouTube.com domain.*” (Bloomberg, 2019)

Thus, a downward spiral is created where the vulnerable and most impressionable populations are exposed to morally questionable at best and clearly manipulative and hateful at worst. Without exposure to anything that says the contrary, or any sort of information that would point out that the content of X video might be inaccurate and not a reliable source of information, the content is taken at face value, believed and internalized. This is how the alt-right movement grew in the past decade and the reason nazism is on the rise. YouTube, in particular, had a huge role here, which recruiters made use of: with knowledge of the political climate and the inadequate perception (and caricaturization) of progressive people and their agendas, people from the alt-right would know that people who don’t know any better would think that liberals are, for instance, intolerant and inflamed on exaggerated topics - this is how the term ‘feminazi’ was coined. So if they criticized these people, and then praised their counterparts, it would not hard for a good chunk of people to buy into their arguments, as they had already been exposed to their initial point (progressive agenda is not taken seriously). And so, when someone would research any topic related to liberal politics, videos that criticized these views would appear in the recommendations. The impressionable mind would then, unbeknownst to them, try to educate themselves more with the wrong sources. Then, by the related topics and underlying graphs, more extreme videos would arise. So the recommendation system would go: “What is equity?” → “Why is equality not achievable” → “Does inequality REALLY exist?” → “Minorities are crybabies” → “Why white people are the most oppressed demographic” → “Everyone hates white people and we need to do something about it” → “Hitler was right”. This transition is not hard to see and has been described in detail by former members of the alt right. From a purely technical point of view, this is because the topics are related (which they are). But this view is extremely reductive and irresponsible of the use and misuse of the technology, and ignores the fact that users are human, not machines. Computers have no ethics, morals, and are not impressionable, but they do not use YouTube. Humans have changing minds, their definition of good and bad changes, are prone to manipulation and are very impressionable, and they use YouTube. The technical argument is irrelevant when the need for accountability is real. In a similar vein but different industry, the recent Boeing 737 crashes are a very real and fatal reminder of how automation needs regulation and accountability from their creators:

“*The problem isn’t limited to airplanes. As automation continues its breakneck expansion, we’re going to see more and more accidents that take place not because something breaks but because humans and complex machinery react in ways that we didn’t—and maybe can’t—expect. “We’re seeing the same accidents happening across different domains,” Malmquist says, from self-driving cars to the Deepwater Horizon catastrophe. “There are a few differences, but in the end, these accidents are almost identical from a systems-theory point of view.”*

*(...)*

*The sheer complexity of those automated systems, however, makes it unclear whether Boeing or any company knows enough to eliminate the risk. Safety experts have begun developing new approaches better suited to the automated world. So far, unfortunately, their uptake hasn’t matched the rate at which these systems are spreading into every corner of human life.*” (OneZero, 2019)

On the human side, polarization is commonplace due to the the inherent limits of written and instant communication, the timeframe of attention span and the way information is processed by the brain. Social media encourages and promotes short texts, images, animations and ‘memes’, all which rely on the impression of the source and not the strength of its content. With this in mind, companies and people make their ‘posts’ as heavy as possible in the fewest words, adding informal language for ease of access to a wider public and impact by relating it to the reader’s world and life: phrases such as “I tried this perfume. I didn’t expect the damage.” are very common, as opposed to “The negative effects of this perfume on human skin”, which would be the unbiased and factual way to talk about the subject. As impression is the goal, controversial or strong language/subjects are usually the way to go for the most engagement, measured in ‘likes’ or replies, which is the goal for most people: social media is the means to an end (promote something), and engagement gets them closer to it. The more a post is shared, the more attention it gets, and the more its message is shared. Responses can be either positive or negative according to the subject, where controversial topics get both equally, but negative responses are unique in their content: instead of casual or intellectual disagreement and the presentation of counterarguments, the most common form of rejection of a message is the diminishing of the idea, infantilization of the creator and, in some cases, bullying. This, while also possible in physical spaces and face-to-face interactions, is most prominent in the internet because of the lack of empathy resulting of the lack of human contact: people don’t see other people, they see lines of text they disagree with. They don’t equate information to an author, and so they don’t try to engage with the information as if it came from a human. This creates more visceral emotions and reactions, which lead to grotesque responses that cannot be avoided even if the human element is explored, as the emotion has already been experienced. Death threats, ‘doxxing’ (the unauthorized disclosure of personal information) and bullying are not only very common but also mainstream enough that they do not surprise. They are almost anticipated.

Despite its immense shortcomings and very questionable implications, social media has been used for positive engagement. Instant communication allows for broader depth and reach, both in participation and membership, by being available to anyone anywhere. This allows for masses of people to join together for a cause, to explore and talk about a subject, participate in specific situations or simply share information. This is why ‘memes’ became so popular: a very specific subject that can be replicated and applied to many circumstances, passed on by mimetic means, has existed in many forms throughout history, but it has never been shared across cultures and states with the same content and context intact as it is right now. The widespread use and/or discussion of some media is talked about with the description of ‘viral’, so described because of its similarity of the contagious stage of a virus. Most of the engagement of any sort of content, when instant, comes from viral campaigns; informal, spontaneous & impromptu organizations are very common and have a higher impact through this phenomenon. The ‘#MeToo’ campaign (a movement where women shared their sexual harassment experiences) and the ALS Ice Bucket Challenge (a challenge aimed at raising awareness of ALS, where people donated money to a foundation) where successful because of their incredible reception, which in turn was possible because of viral engagement.

With the traditional frame of civil societies as hallmarks of democracy also came the implication that they were only possible in specific circumstances. While this led to the discussion of ‘uncivil’ societies (civil societies who make use of undemocratic means or values), it also had the effect of sidelining any group that exists outside of a political state or in a non democratic state. China, for example, has a civil society environment that is markedly different from other countries (particularly, western countries): if these were analyzed from a western perspective, they fail to live up to the expectations that democratic civil societies have marked. This does not mean they are not civil societies, but rather, that the definition of a civil society in terms of democracy is extremely limiting. In the same vein, digital civil societies are very different from the ‘real world’ counterparts. Plenty of the associations in the internet do not have anything to do with any political element, nor do they necessarily express support for democracy or make use of it (since some members might come from non-democratic countries). Take, for example, the group Anonymous, a group that defines it itself by very simple ideals: anyone who says they are part of anonymous is part of it, just as long as they remain anonymous. There is no intent in mind, membership requirements, or reason for being. As a matter of fact, very different and conflicting activities have been claimed by Anonymous members without other members in the group being none the wiser. The group is most famous for their hacktivism (although they do more than that, as there are members that do not engage in this activity) and work with WikiLeaks, where they illegally obtain access to government servers to disclose sensitive information they think the wider public should have access to (with the intent of holding these governments accountable for their actions), or hack and obstruct the practice of individuals and organizations that go against internet neutrality and associated topics. This is the digital equivalent of a protest, but it has much more power than one because of the very real, very effective disruptions it causes to its targets. A stand-in protest can be ignored; thousands of servers down and lack of access to products can not. This lead to the eventual and highly controversial imprisonment of members of ‘LulzSec’, a faction inside of Anonymous that led most of these activities, with the argument that they had gained access to the servers through illegal means (some members of LulzSec pleaded guilty to this, while others pleaded innocent). This would be the equivalent of imprisoning protesters for civil disobedience (also highly controversial), where the authorities focus on the technicalities of their actions instead of their goals and motives.

While LulzSec was heavily invested in hacktivism, most of Anonymous did not, and at times some factions would engage in activities that seem to go against the development of democratic values. When questioned on their actions, some have responded that they thought ‘it would be funny’ (this was the reason of the name LulzSec) and did not have a particular intent in mind beyond the initial impact of their activities. At times their actions promoted conflict, and in others it called for the resolution of one. This contradictory coexistence exemplifies the dual nature of the internet, where one same tool can be used for good and evil.

Civil societies have many flavours and forms. From civil responsibility and government accountability to hobbyists groups and merchant associations, these congregations can spring up anywhere, even on non democratic environment. Just as their ‘uncivil’ counterparts, digital civil societies are often the source of disagreements between scholars, despite evidence showing their clear impact on society and democracy. In a way, the conflicts that arise in the internet are attempted to be solved by the internet itself. Like the snake eating its own tail, societies in the internet are constantly in battle against each other, at times crossing into presencial events. The incredible communication possible through these platforms make them a breeding ground for all sorts of points of view; conflict will arise when they collide. Just as well, parties who understand both sides and act as intermediators are also very common. The very space itself could be argued to be a vehicle for conflict resolution, as the exposure to contrary points of view educates observers of all sides of the argument and invites participation. Ultimately, the internet is a tool: how and for what it is used is up to the user. Both conflict and conflict resolution are possible, encouraged and present.

References:

* Munroe, R. [*Duty Calls*](https://www.xkcd.com/386/), XKCD
* Ye, Z. (2003). [*China’s Emerging Civil Society*](https://www.brookings.edu/research/chinas-emerging-civil-society/), Brookings
* Borges, J.L. (1962). *Fictions - Tlon, Uqbar, Orbis Tertius* [Short Story]
* Hong, S., & Kim, S. H. (2016). [Political polarization on twitter: Implications for the use of social media in digital governments](https://www.sciencedirect.com/science/article/pii/S0740624X16300375). Government Information Quarterly, 33(4), 777-782.
* Hong, S. (2016). [Political Polarization on Twitter: Social media May Contribute to Online Extremism](https://scholar.harvard.edu/sounman_hong/political-polarization-twitter-social-media-may-contribute-online-extremism), Harvard.
* Beren, M. (2019). [YouTube Executives Ignored Warnings, Letting Toxic Videos Run Rampant](https://www.bloomberg.com/news/features/2019-04-02/youtube-executives-ignored-warnings-letting-toxic-videos-run-rampant), Bloomberg
* de-Wit, L,, Brick C., van der Linden, S. (2019). [Are Social Media Driving Political Polarization?](https://greatergood.berkeley.edu/article/item/is_social_media_driving_political_polarization), Greater Good Berkeley.
* Lee, C., Shinb, J., Hong, A. (2017). [Does social media use really make people politically polarized? Direct and indirect effects of social media use on political polarization in South Korea](https://www.sciencedirect.com/science/article/abs/pii/S0736585317305208), Science Direct.
* Michael J. Jensen, James N. Danziger & Alladi Venkatesh (2007) [Civil Society and Cyber Society: The Role of the Internet in Community Associations and Democratic Politics](https://www.tandfonline.com/doi/abs/10.1080/01972240601057528), The Information Society.
* Wise, J. (2019). [No One Knows How Dangerous Boeing’s 737 Max Actually Is](https://onezero.medium.com/no-one-knows-how-dangerous-boeings-737-max-actually-is-d4256239af40), OneZero
* Venkatesh, A. (2009). [Civil Society and Cyber Society: The Role of the Internet in Community Associations and Democratic Politics](https://www.tandfonline.com/doi/abs/10.1080/01972240601057528), The Information Society