

Patrick Louis

# INTERNET

Medium for Communication, Medium for Narrative Control

# Internet

Medium for Communication, Medium for Narrative Control

Patrick Louis

Published online on [venam.nixers.net](http://venam.nixers.net)

© Patrick Louis 2021

This publication is in copyright. Subject to statutory exception and to the provision of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of the rightful author.

First published eBook format 2021

The author has no responsibility for the persistence or accuracy of urls for external or third-party internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

*Enter with the intention of growing as an individual.*

This page intentionally left blank.

# Contents

<b>Introduction</b>	<b>7</b>
<b>The Artifacts and Spaces</b>	<b>9</b>
Defining and Understanding Propaganda, Influence, and Persuasion	10
Social Media and the Democratization of Speech . . . . .	18
Data and Metadata: Personal Data and Models . . . . .	24
Memes and Cults . . . . .	29
<b>The Actors and Incentives</b>	<b>40</b>
New Economies: Information Economy, Attention Economy, Data Economy, Surveillance Economy . . . . .	41
Internet, in Between the Corporate, Private, and Public Spheres . .	50
State Actors: PSYOP, Narrative Warfare, and Weaponized Tech . .	59
<b>Biases and Self</b>	<b>68</b>
Cognitive Biases . . . . .	69
Cultural Ambiguities and Insecurities . . . . .	73
<b>The Big Picture</b>	<b>79</b>
The Formatted Individual . . . . .	80
Truth and Trust Crises . . . . .	89
Mass Hypnosis or Mass Psychosis . . . . .	98
<b>Adapting</b>	<b>104</b>
Free Market, Let it Solve Itself . . . . .	105
Legality, Transparency, Accountability, the Nations Intervene . . . .	113
Technical Solutions, Wars and Patches . . . . .	126
Education, Literacy, and Reality . . . . .	131
<b>Conclusion</b>	<b>138</b>
<b>Bibliography</b>	<b>139</b>
<b>Index</b>	<b>159</b>

# Introduction



Peter Apian, Astronomicum Caesareum (Ingoldstadt, 1540)

To no one's surprise, the internet has permeated all aspects of our lives. All other means of communication have dwindled in comparison, even though the technological behemoth is relatively young (around 50 years old as of 2021). Worldwide, according to statistics from 2019, people spent an average of 2 and a half hours a day on social media. The top place goes to The Philippines with 3h53min per day.

This raises an iceberg of loaded questions.

At the top: *How controlling is the internet today?*

Or, asking in reverse: *How does internet, as a new vector of communication, let different actors control us? How is the internet changing the way communication works and, indirectly, how we think?*

These are broad questions and there are plenty of sub-questions underneath. Indeed, we keep hearing in the news about social media, extremism on the rise, and a salad of convoluted keywords thrown in articles trying to rationalize all this.

Is there really an information war?

What are the elements of it?

Who are the actors?

What's the relation with social media?

Is it related to all the conspiracy theories we keep hearing about?

Is journalism dying?

What is the attention and data economy?

Are we all part of a giant hypnosis experiment?

More importantly, can we, and should we, do something about this?

Like many of you, I've asked myself these questions countless times, got buried in a mountain of headlines and news articles selling shock-value pseudo-deciphering. I temporarily felt clear-headed but quickly got back to a muddy state of comprehension.

Thus, I've set myself to consume all the literature I could find, peel it, parse it, organize it, categorize it, hone it, filter it, etc.. So that I could, at least partly, remove the haze surrounding the topic.

This is going to be my attempt at answering how the internet changes communication regarding narrative control. My own mini internet studies.

Here is the rough plan of our exploration.

- **Part 1: *The Artifacts And Spaces***  
In this part we'll describe the important artifacts and places. Going over these essential, but basic, pieces is mandatory to understand how they come into play as tools.
- **Part 2: *The Actors and Incentives***  
In this part we'll go over how the previous elements are put into work by the different actors, who these actors are, what are their incentives, and the new dynamics.
- **Part 3: *Biases and Self***  
In this part we'll try to understand why we are prone to manipulation, why they work so effectively or not on us, and who is subject to them.
- **Part 4: *The Big Picture***  
In this part we'll put forward the reasons why we should care about what is happening in the online sphere. Why it's important to pay attention to it and the effects it could have at the scale of societies, and individuals. This part will attempt to give the bigger picture of the situation.
- **Part 5: *Adapting***  
In this concluding part we'll go over the multiple solutions that have been proposed or tried to counter the negative aspects of the internet.

Get ready because this is going to be a long ride!

## **The Artifacts and Spaces**

## Defining and Understanding Propaganda, Influence, and Persuasion



René Descartes, *Traité de l'homme*

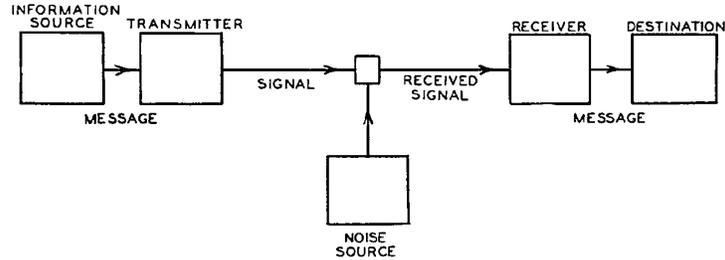
- Communication
- Influence
- Persuasion
- Propaganda
- Types of Propaganda
- Administering
- Reinforcement, Anchor, Hook, Imagery
- Ethics and Issues of Identification

Our journey begins with three terms: propaganda, influence, and persuasion. To most, they sound like synonyms, but each convey a different concept. Like any form of communication the internet can be used as a channel for them. What does communication consist of?

The very broad domain of communication studies — with multiple sub-disciplines such as journalism, film critic, public relation, and political science — often use a simple reductionist model called the Shannon–Weaver model of communication.

The model has 7 different concepts: Information source, Encoder, Channel, Decoder, Destination, and Noise. In our case, the internet is used as the pipe that conducts the signal, the transmitter and receiver are the chosen form of media (video, text, audio), and the information source and destination are the people and algorithms at both ends.

This model is not complete as it does not take into consideration the personalities of the persons involved, nor context, history, time, or any other clues that



Shannon-Weaver’s Model of Communication Diagram

make communication complex. Moreover, it is limited to one-to-one scenarios and doesn’t cover one-to-many.

Regardless of these flaws, the model gives a generic picture of what communication is: It is about sharing meaning — a message — through the exchange of information via symbols that have perceived meanings on both ends.

The Shannon-Weaver model is a great starting point to see what needs to be done so that the conduct becomes more reliable, reducing uncertainty. That is, we need to keep in mind the qualities of context, sender, intent, message, channel, audience, and response. Concretely, the more the exchange the less the ambiguity, both parties converging towards a common point, common interest, or focus.

All this to say that the internet is a medium for transporting information. Just like the printing press lead to novelties, change in thoughts, and brought doctrines to the public like never before, the internet has its own characteristics but can only be defined by what we use it for.

For now, let’s pause and go back to what propaganda, influence, and persuasion are.

Influence is a generic word to convey that someone’s decisions have been affected by something. Influence is passive, the person makes the decision themselves unconsciously. It can happen with or without any direct communication (verbal or nonverbal). It is a spontaneous mix of inner motivations and environment. Consequently, it is rarely, if ever, controlled by another entity’s will unless this entity has full control over the environment.

The nudge theory argues that an entity can influence people through positive or negative reinforcement, indirect suggestions. However, the long term effects of these suggestions are highly contested as they get mixed with other environmental factors like peer pressure and social norms.

An example of influence is product placement, where a product is desired based on its indirect association with a portrayed lifestyle that the viewer would, in theory, like to obtain.

Persuasion, on the other hand, is based on a two-way interaction. It is often

used in negotiation when one party or many parties want to take over the other, imposing their point. The difference with negotiation is that the core of the message never changes, it is not about resolving a common conflict but gradually convincing someone.

Persuasion is thus transactional and voluntary. The party that wants their message to come across has to bridge through the individual psychological process, to exchange ideas freely and openly so that the other will be convinced. In persuasion there is a back and forth between persuader and persuadee, the persuader adapting, shaping, reinforcing, changing the message at each iteration to make it more appealing depending on the persuadee's responses.

If the persuasion succeeds, it should result in a reaction such as "I never saw it that way before".

Persuasion can be verbal or nonverbal. It can either look like a consensual dialogue to reach an understanding, or look like strategic information or awareness campaigns that appear one-way but are still using a feedback mechanism to hone the message. This former is called Organized Persuasive Communication (OPC), and refers to all organized persuasion activities (advertising, marketing, public relations, organizational communication), but the term can also refer to more manipulative means.

In both these cases there is a free flow of information and the persuadee is fully aware of what is happening.

People are reluctant to change and so to convince them the persuader has to shape the message in a relatable way to something the persuadee already believes, or use lies and tactics morphing the facts.

This means persuasion can take a manipulative form, which may or may not be consensual. For example when someone is persuaded under false pretences, incentivized via promises, provided extra benefits, or coerced through threats or actual infliction of costs (including withdrawal of benefits).

Propaganda goes in that manipulative direction. It is exclusively a one-to-many massive persuasive strategy that is deliberately trying to shape perceptions, cognitions, and the direct behavior to achieve the desired intent of the propagandist.

Historically, propaganda didn't have the same meaning it has today. It meant "to propagate" or "to disseminate", but the term has changed over time as it got attached with the dissemination of information by governments for particular purposes.

Purpose is what differentiates propaganda. It is always meant to be targeted at a specific group, category of people, or society with the goal to push them in the desired direction. This objective is often linked to institutional ideologies, that is why we call propaganda *activated ideology*.

This means it is inherently advantageous to the propagandists, and their ideological fellows, but not necessarily the recipients. In some cases, it is arguable, and depends on the viewer, if the message is propaganda or education.

Propaganda doesn't shy away from using whatever means available to inculcate

the message. It isn't based on mutual understanding, omits or hides information, uses deception, uses manipulation, frames issues, coerces or deceptively coerces, distorts, lies, overemphasizes, and misdirects. Anything goes, as long as the goal is reached.

The message is crafted in a deliberate way to support a viewpoint, a narrative, a goal of an ideology.

This is why propagandist consultants are often called "spin doctors" or "spin-meisters", reinterpreting the events under a particular perspective.

The corollary of propaganda is censorship. The entity that wants to control the perception of its ideology silences any message that doesn't fit. It achieves the same purpose by, not filling people's mind with approved information, but preventing them from being confronted with opposing points of view.

That is why propagandists require control of information flow so that they can manufacture it. This allows them to select the current agenda — telling the public what is important and what isn't. Or to frame problems, influencing how the public pictures a situation, creating the images and opinions that go along the ideological goal. The propagandists try to control the media as a source of information distribution and to present distorted information from what appears to be credible sources.

Indeed, it is also imperative that the message should be packaged in ways that conceal its manipulative persuasive purpose, as we'll see later.

Another interesting typical aspect of propaganda as communication is its heavy use of symbols and association. That is in direct relation to its institutional and ideological root. For instance: justice, liberty, devotion to a country, etc.. Symbolism is also heavily employed in advertising propaganda to sell products as ideologies and ways of living.

Wherever you look and ask, all domains of research and work that touch propaganda dismiss their association with it. Public relation dismisses it as consensual and not manipulative, and the same in the advertising industry. The studies of propaganda are filled with euphemism, diverting attention, using the techniques they are themselves describing.

The historian Zbyněk Zeman categorizes propaganda as either white, grey or black, but there are other categorizations too.

White propaganda is when the message is sent from an official source and the intent is more or less clear. For example, a message on TV by the president of a country.

Black propaganda is when the message conceals the source and intent by making it seem as if it emerged from the same people, group, or organization it is targeting. Obscuring the identity of the originator is done to make the message more credible, giving the impression it comes from the people it's trying to discredit or manipulate. It is also used for diplomatic reasons to hide government involvement.

For the propagandist, this is the type that is safer and has greater persuasiveness.

Grey propaganda lives in between, it is a message coming from an ambiguous or non-disclosed source, and the intent isn't known. This could be a rumor or a message based on unnamed insider's info.

Counter-propaganda is the reaction to propaganda. It differs from it in how it is defensive, based on facts and truth, clear (understood by everyone), calling out logical fallacies. It is most often administered as a white propaganda. Propaganda can only be countered effectively if the counter-propaganda acts quickly to overcome its damage. Propaganda uses an anchor, as we'll see, and it needs to be dismantled as soon as possible. That means the older the propaganda the more it will be deeply rooted in people's mind.

Self-propaganda is a type of propaganda where someone deliberately tries to convince themselves of something, even if irrational. This is akin to a Stockholm syndrome in some cases.

Sub-propaganda refers to anything that isn't direct propaganda but to ways to keep the door open for future opportunities of propaganda.

Within this category we find *promotional culture* that is used in marketing and other domains. It consists of promoting commodities, celebrities, politics, civil society, social cultural traditions, economic ways, etc.. It is the salesmanship of a culture and thus cobbled with direct and indirect marketing means.

Computational propaganda is, according to Phil Howard, "*the assemblage of social media platforms, autonomous agents, and big data tasked with the manipulation of public opinion.*"

Computational propaganda can be directed by agendas or not. It could passively happen because of the incentive of the algorithms on the platforms — usually social media and thus views and clicks as we'll see in other sections.

Propaganda, like any other type of communication, depends heavily on the environment and context in which it is moving.

Another related concept is persuasive technology, whenever a digital platform has full control of the environment of a user and attempts to change their attitudes through social influence and persuasion techniques. This consists in creating an environment that guides the person to perform certain actions and not others, inciting them through different means like social feedback, extrinsic or intrinsic motivations, and positive and negative reinforcement..

When it comes to administering persuasion and propaganda, the process is intuitive: Choose the target group and message to transmit. Choose the media form, the media shell, depending on how easily it can spread. Pack the message material in the shell, and send it towards either the mass/group, or towards specific individuals that could spread it further. If an opinion leader spread it then their credibility, expertise, trustworthiness, and attractiveness with respect to the target group should be analyzed to match the message.

Then ensues a series of iterations to polish the message through reinforcement, repetition, targeting opinion leaders through indoctrination, and the addition of new psychological techniques, manipulation of the message, emotions, and

logical fallacies appropriate to the target audience.

If the propagandists' or persuaders' goal go to the contrary of the habits of the audience, it will be difficult to achieve and will require awareness and information related to behavioral change and predictors of behavior of the target audience.

That is, the message, to have its effect, will need to be adapted and employ tactics to resonate with the audience.

The message shouldn't be imposed, instead the recipient should feel it flow effortlessly within themselves. Any propaganda shouldn't look like propaganda to the target audience. "*Propaganda is most effective when it is least noticeable*". The change will need to be self-imposed. This is similar to the nudge theory of reinforcement, it should appear as influence and not propaganda.

For that, the message should seem to give expression to the recipient's own concerns, tensions, aspirations, and hopes. It must identify with them, this is what we call the *anchor*.

This anchor activates the ideology of the propagandist by tying down new attitudes or behaviors along with existing ones. It is the starting point for change because it represents something already widely accepted by potential persuadees — it is the path of least resistance.

These anchors can be categorized as either belief, value, attitude, behavior, and group norms.

An anchor of belief is one of the best anchor, and the stronger the belief of a receiver, the more likely they will attach to the propaganda goal.

A value is a kind of long-term belief that is not likely to change. It is hard to use as anchor because these are unwavering and so might conflict with the propagandist goal.

An attitude is the readiness to respond to an idea, object, or course of action. It is a predisposition that already resides within the receiver. The propagandist can activate the predisposition to further achieve the goal.

A behavior or behavioral pattern is a clear indication of how receivers are currently acting and often predicts future behaviors.

Group norms are beliefs, values, attitudes, and behaviors derived from the membership of the receiver in a group. The propagandist can use this tendency to conformity to make the message organically move laterally within the group.

A concept similar to the anchor is called the *hook*. It differs from the anchor in that it is based on a unique event or idea that is constantly repeated to amplify its effect.

The hook is generally a story which central element makes it newsworthy and evokes strong emotional responses, making it stick to memory. It could be fabricated (such as deep fake), misleading and creating doubts, or real, but most importantly it should spread quickly and inundate all conversations on a topic. The hook is then attached with whatever piece of information it was packed with.

Hooks and anchors regularly use typical imagery to reach the ideological goal. For example, portraying the enemy as a baby killer.

The compaction of big ideas into small packages that can be distributed effortlessly is a must. This can be done through emotional wording, hook-like stories, symbolic images, and impactful videos. This is a form of portable philosophy created through repetition, emotions, and stories that lead to new meanings. Notably, when using symbols, words, and images, that already live in the collective imagination, they will bring with them a baggage of feelings, concepts, and ideas. Think of all the recently rehashed tropes in media like movies, songs, images, and news. The use of strong wording will color the message, creating an association in the collective memory: genocide, patriotism, invader, victim, democracy, anarchy, enemy, confrontation, massacre, coup, radicalization, etc..

To spread further and faster, the anchors, hooks, and imageries must all interpolate and abuse our own confused cultural code. They work by exploiting issues we haven't adequately addressed as a society. That is why people show strong responses to messages that are linked to injustice, outrage, partisanship à la we-vs-them, and controversies. We are more likely to react to things we don't agree with.

From economic inequalities, race, nationalism, gender roles, sexual norms, etc.. It doesn't matter which side of the issue people are on, the message will be spread and will provoke a reaction — if this is the goal of the propagandist. It could also be fabricated controversies, seeding doubt on purpose, making it seem like we're still on the fence, ignorant (the domain of agnotology). The propagandist expertly triggers hope, satisfaction, pride, enthusiasm, but also fear, anxiety, anger, outrage, and disgust.

Let's take a look at how Robert Cialdini details 6 principles of persuasion:

- Reciprocity: People feel the need to give back to someone who provided a product, service, or information.
- Scarcity: People want items that they believe are in short supply.
- Authority: People are swayed by a credible expert on a particular topic.
- Consistency: People strive to be consistent in their beliefs and behaviors.
- Likability: People are influenced by those who are similar, complimentary, and cooperative.
- Consensus: People tend to make choices that seem popular among others.

These go hand in hand with what we described so far and also reminds us of the conveyor of the packed message. We should pay attention to the credibility of the source, if the source is revealed.

Yet, a trick in propaganda is to keep confirming what you said, to never argue and assume the truth. Our mind is wired to accept and believe what others say as true, especially if not contradicting with any prior belief or value.

The rule of thumb is that the message shouldn't create any cognitive dissonance but instead build a world that feels real to the recipient. To create a cohesive cosmology of meanings, to sell a coherent memorable story.

However, propaganda still denies the distance between the source and audience

because it puts the ideology first.

We'll dive in the psychological aspects in another part. For now, this should have created a strong foundation to understand influence, persuasion, and propaganda.

The exact identification of what can and should be considered propaganda is debatable and extremely hard to do. Some researchers have attempted to create a framework to discern manipulative persuasion from consensual informational and dialogical ones, but this is hardly applicable to the real world. And, as we said, propaganda could be considered education in the eye of some people.

When it comes to ethics, the subject of children indoctrination comes to mind. Children are the most vulnerable targets of propaganda as they haven't built strong defenses against them. They are the least prepared for critical reasoning and contextual comprehension and thus are impressionable. Their mental world is in the process of being built and is easier to mold. There is no strong forces to oppose the propagandist goal.

On that note, it is subjective whether certain types of persuasions and propagandas are ethical or not. Propagandists are driven by ideologies, and consequently strongly believe that all means are necessary. As with anything related to ethics and moral, it differs based on personal judgement of the actions. For some people, it is ethically wrong to employ any subterfuge or tactics to reach a goal. For others, it is not about the tactics but whether the goal itself is right or wrong.

There's a lot to be said on the black and white division of ethics, but we'll leave it at that because the world is inherently nebulous.

This concludes our review of propaganda, influence, and persuasion. We've taken a look at the basic idea of communication, the packing of a message. We've then defined influence, persuasion, and propaganda, with propaganda being a type of persuasion that is one-to-many, manipulative, and driven by ideology. We've seen different types of propaganda and their definitions such as black, white, grey, self-, and others. Then we've seen how this package can be administered effectively through the person or channel carrying it and the actual shell of the message. This message will be successful if it doesn't conflict with the receiver, if it is reinforced, uses an anchor, a hook, or strong imagery. The message will spread further and faster if it triggers strong emotional responses, especially something people feel they have to stand against. Finally, we've glanced at the issue of identification and the ethics concerning propaganda and the most vulnerable.



According to a Facebook's statistics, there are 2.8 billion monthly active users on the platform. Pew research also shows that, in 2019 in the USA, Facebook was used by 69% of adults, while YouTube was used by 73% of them. Additionally, Worldwide statistics of the same year (2019) show that people spend on average 2 and a half hours a day on social media. These massive penetration rates are clear indicators of how social media have taken part in the lives of many.

The platforms rely on a network effect to attract and create social hubs — The more the people on a platform, the more others will want to join it. This is the inherent social aspect, that's why we also call them "social networks".

Consequently, any information circulating on the popular social media could benefit from exposure that no other medium has.

The exposure is complemented with an instantaneous spread, a fast pass-it on effect. The engagement of users allowing the fast sharing of information. Quickly creating an amplification of the message, letting it travel through social circles that would've never been reached before — a wider transmission that breaks distances.

Another fitness criteria is how enduring and suitable the storage media is. The internet has a long-lasting memory, by the time the message is out it will have been copied and stored in multiple places. It will be almost impossible to erase.

These three criteria: exposure, speed, and memory, break previous media standards. However, to exploit this new medium successfully the information sent through it needs to adapt symbiotically to the ecosystem and niche in which it exists. If it is hostile, the information won't be transmitted.

For example, the message will need to take in consideration the augmented Chinese Whisper effect taking place due to the speed and social aspects.

Another component that needs to be considered in the social media space, is the infobesity, also known as the infoxication phenomenon. The information is long-lasting, as we said, and accumulates over time. The users of the social media are overloaded with them.

The senders of mass messages will have to keep this in mind and craft their messages appropriately to penetrate social media. Indeed, the people on the platforms will never be able to consume all that is presented to them, and have to be picky with what they choose to process.

These are all indicators of the scale that the internet platforms, particularly social platforms, have and their potential use.

Most importantly, they have dethroned traditional mainstream media gatekeepers and allowed the common people to reach a wide audience, bypassing filters and safeguards.

In the past, there were two main ways to get information: through peers or through traditional media.

With peers, we'd learn about the world events through their stories, rumors, and anecdotes.

Traditional media, as the only other source, were subject to different types

of manipulation. To protect the public and stand as gatekeepers of truth they erected journalism standards, free press, fact checking, and other types of regulation present in multiple countries.

At least that's the theory. It remains ambiguous if traditional media are still influenced, controlled, and driven by ideological stances or corporate incentives.

Nowadays, we are presented with an alternative: the ordinary person as a media producer and filter. On social media, we aren't subject to the standards and safeguards that mainstream media have.

People democratically filter and promote the news, ideas, and information that they consider important. The majority decides what is relevant and what isn't. The phenomenon is similar to conversations with friends being converted from one-to-one into one-to-many, an amplification of decentralized voices. These voices are driven by an appeal to emotions and popularity, and not by reason, deliberations, qualifications, backgrounds, incentives, history, or others.

These are the messages that pierce through.

It is now frequent that mainstream media accentuate the legitimacy and credibility of social media by regurgitating their news from the different platforms. This can be interpreted as a confirmation and encouragement for participating on them.

The generation and distribution of media has been made effortless. Anyone can easily take part in it. This is the will of the actors owning the platforms, which we'll see in another section.

The availability of digital equipment makes it a breeze to edit, write, capture, record, and film content.

The public is socially rewarded for their engagement, be it sharing, commenting, producing, or distributing. The usual social rules are in places such as wishing for fame or conforming and belonging to a community. We'll also discuss in depth the psychological aspects in another section.

In sum, the public discourse on social media is a new place where the creation of narratives about events happens, and where they are discovered.

The digital platforms are also social places used for cultural, personal, and intimate relationships. This combines senses of trust and familiarity along with individualization and personality.

People maintain *profiles* on social media, facades of their personality that they mold with the aim of displaying it to an audience. The platforms normally allow for the customization and individualization of what can be interacted with, is recommended, and the style and types of messages received. It goes both ways: the person forms the virtual persona they want, and the digital platform assists in surrounding that persona with an environment that will foster it within boundaries.

Practically, that means the social media user will have personalized news and media, and interact with others, according to how they portray themselves.

Furthermore, the individualization, along with the fact that other users on the

platform might already have social bonds with the person outside the digital space, induce feelings of trust and familiarity. However, this is complemented with an inability to establish new organic social bonds through social media — we aren't able to connect deeply. We feel closer, yet further. Familiarity is also felt through the repetition of the customized messages targeted for the particular persona.

As with any type of social place where communication happens, conversations will touch topics that conflict across cultures. Just like mainstream media newspapers could be leaning toward different points of view, now everyone on social media reiterate their ideologies. An outer expression and clash of the inner confused and unaddressed stances of our societies and cultures.

Unquestionably, the most favored topic, the one driving the most engagement, is politics. Social media are the hubs for political discussions. According to Pew Research Center, 39% of adults in the USA used social media solely for political purposes. Interacting with media that has political meaning, which translates into “liking”, sharing, reposting, discussing, creating political posts.

Interestingly, social media are positioned between socialization, entertainment, and information consumption. For a vast majority of users political interaction has turned into infotainment, information sharing as entertainment. A caricaturization of politics, reducing political acts to quick and easy bona fide participation on social platforms — What is called hashtag activism or slacktivism.

Along with the overload of information and the democratic filter, users will indirectly encounter all types of conflicting ideas while browsing to entertain themselves. These having spread exactly because they interpolated the engagement of so many others.

The types of information that usually stand out are the ones that challenge our ideologies and culture, as we said. These types of messages can pierce through.

Some theory implies that because divergent views exists at the same time on social media, this latter is akin to low-context societies.

High-context mode are the communications that happen with an inner-group, including the subtle codes, traditions, and meanings. While low-context mode are the communications that are straight forward, reducing ambiguity, flat, and global.

This can be what some call an *information society*, a society in which creating, manipulating, and sharing of information is central. The people being part of this society would then be digital citizens.

We are having an incredibly difficult time adapting to this new medium, now that everyone has an equal voice.

We still refuge ourselves in different cocoons that collide in parody-like confrontations with one another. Again, a reflection of our own cultural weaknesses, our cultural insecurities.

These bubbles then can only be pierced through by more extreme content and ideas that will travel further. That means we are moving the Overton window — the ideas tolerated in public discourse. Fringe ideas on social media are the ones that are heard the most and might be accepted as normal. The medium having voted democratically that this was what the majority voted as relevant.

Obviously, the votes are not all done by real human beings, the platforms have their share of responsibilities and reasons to promote certain types of discourse that drive engagement, as we'll see soon.

This reminds us of the nudge theory and persuasive tech we've learned about in the previous section and how it could only be achieved when an actor has full control of the environment; This is the case with most social media. They can, and do, deliberately create digital environments that users feel fulfill their basic human drives.

Hiding the actors affect the messages greatly, this is done in two ways: anonymity and automation.

The use of persona that aren't attached to real individuals let people express themselves without restraints. This attracts bitter views and clashes, as people can now break the accepted cultural codes.

These anonymized profiles can then be automated by algorithms, what we call bots, and exchange with other social media users to promote a message. Consequentially, cheating the democratization of speech and artificially creating a public opinion by giving importance to selected ideas.

We referred to these autonomous agents as computational propaganda in the previous section. Statistics show that around 40% of the traffic on social media is composed of these autonomous agents. We'll explore later the incentives of the actors.

Let's finally mention that there are different types of social media platforms. Some have specific rules, some are only used to share a single type of media, some are centralized, some are decentralized, some are anonymous, some require identification, some are more fringe than others, etc..

Social media have all the essential components we've described, but they are mainly guided by the platforms themselves. They are new instruments, new tools in our hands.

That is why some persons start to see social media as public utilities, even though they are far from it. A public utility being "an infrastructural necessity for the general public where the supply conditions are such that the public may not be provided with a reasonable service at reasonable prices because of monopoly in the area." For that, a governing body will need to be erected and have monopoly over the social media in place and justify them being a necessity.

Overall, the medium reveals more about the people than about itself. It is how we use it that matters and the confusion we feel could be a manifestation of our own confusion. Or is it?

This concludes our review of what social media are as new communication channels. We've first seen its efficiency characteristics: huge reach, high speed, reliability. Then we've contemplated how it has broken the walls of the mainstream media gatekeepers and putting the keys of the castle in the hands of the common person. Later we've seen how it intertwines a social space with a media space, including all our cultural issues and how we want constant entertainment. Next, we've described how hard it is for the information to pierce through and how that increases extremeness in the messages to actually reach us. And finally, we've discussed anonymity and automation as ways to cheat the pseudo-democratic process that is supposed to happen on social media to elect what is important and what isn't.

## Data and Metadata: Personal Data and Models



W. Blake, Death Door, from: Gates of Paradise 1793

- What is Personal Data
- How is it Extracted, What's its Value
- Information Flow Analysis
- The Power of Models

The internet is littered with nuggets of information, some made of gold and some worthless. From this mine we can extract meta-information, inferences that can lead to more lucrative valleys.

Two of the most talked about are personal data and models, also known as statistical trends visualizations, big data analysis, and predictive studies. Let's take a look at what is personal data, where and why people share them, why they're valuable, and how they can be used with different types of models.

In another part we'll focus on the actors and consequences.

Personal data is any information that can be used to directly or indirectly identify a person, an attribute currently attached to them, a behavior, a preference or interest, personal history, anything.

These include things such as name, phone number, address, email, schoolbook, credit scores, geolocation, travel logs, interests, information about past purchases, health records, insurance records, online behavior, etc..

We call the person to which the personal data belongs a data subject.

Information gathering is omnipresent, we are deliberately, or not, leaving trails in the digital space. On a daily basis, in modern society, through our regular actions, it is inevitable that our activities will generate data that is collected, which may or may not require our permission or knowledge.

As we'll see later, the online services and their sub-contractors benefit from this exchange process, relying on the brokerage of big data about their consumers.

The digital world is interwoven with our physical world, we are incentivized to enter information to access services and utilities. Everything is being datafied, anything that can be turned digital will be, including us from birth till death. Are we an information society?

Data collection has been normalized, and we will see the general effects of this in another section. This is justified by the advantages this can convey such as having an optimized service.

There are five places where data gathering happens: casual online browsing and searches, social media, third party marketing, smart widgets, and traditional data repositories.

The biggest collectors are internet-based navigation sites like Google, Yahoo, and Bing. Apart from the data source coming from their search engine services, these companies have a broader business model where they offer tools such as emails, document editors, file storage facilities, and others in which they gather information about users.

These are used for targeted ads. For example, Gmail, a Google owned email service, will direct their marketing campaigns based on the type of mails a user has exchanged.

Likewise, massive amount of data is collected via social networking websites and mobile applications like Facebook, Twitter, LinkedIn, etc..

Users on these platforms either voluntarily communicate information with a public audience by messaging them, or indirectly share their behavioral patterns and preferences by filling a persona — The persona having meta-information stored and used by the platforms and advertising partners.

The data subjects might be lead to believe they own the data they generate through their activities on the platforms, however depending on the legal policy of the services and the legislation in which they reside, it is often not the case.

Third-party marketing providers are good source of consumer data. This includes companies such as KBM, Acxiom, and Equifax which have built consumer databases with information including wage data, occupations, past purchases, transactions, etc.. It is frequent that these third-parties partner or sell their information database to other entities.

In this category we also find credit card companies that might share processing data.

Yet another source of data are all the connected widgets. That include devices such as smart watches, smart doorbells, facial recognition cameras, fingerprint scanners, toys, and others. These could connect to smartphone applications, or

directly to the internet, and the data might be forwarded to a third-party by the parent company.

Finally, the classical places where we find data collections are the traditional repositories. These are the ones that have been used since forever by insurance companies and that contain information such as credit scores, vehicle registration records, medical records, and other official and non-official knowledge.

Each piece of information in itself might not be valuable but the aggregation and processing makes it so. It's quantity over quality, and the more data the more the approximate improvement.

This data confers a huge advantage to companies that use it compared to competitors that don't. Like a GPS using multiple points to find a spot, the data allows for finely grained personalization of services and data-driven decisions. Companies can understand customers needs and wants, and have better marketing, products, and services.

Some argue that the companies might even know more about you than you know yourself.

Most companies and industries already used similar knowledge base in the past for marketing, as a result they only supplement their existing internal source with the external ones they can buy.

This gives rise to a business model, a new type of economy, in which personal data is commodified, gathered at all costs to be resold later to these companies. We'll get back to this in the next part.

This type of business is lucrative, there is a lot of money involved. Simply taking a look at names such as Alphabet, Amazon, Apple, Facebook, and Microsoft that have insane profits racking up over \$25B each year should give an idea. Or even looking at commercial consumer database owners such as Acxiom that makes sales of \$1.13 billions and have customers such as big banks, investment services, department stores, and automakers.

This data is pieced together, shared, aggregated, and monetized, fueling a \$227 billion-a-year industry. This occurs every day, as people go about their daily lives, often without their knowledge or permission.

There is so much money involved because the return-on-investment for firms that have embraced it shows that it works. In an ever-moving world, it is always a leverage to know about your consumer target and predict trends.

The data isn't available to everyone though, and the companies owning them aren't keen on letting go of their business. Moreover, there are moral, ethical, and legal regulatory concerns that are starting to develop around the topic.

Practically, this gathered data needs to be processed to be used by companies or other entities. That amounts to collecting, structuring, organizing, storing, sharing, and modeling the information.

The digitalization allows not only to deduce direct information from the data

(such as personal interests in a topic), but also indirect ones like the flow of information. For example, it can allow knowing which persons are more prone to interact together. How data moves is information in itself.

This can help to know via clear metrics if a message was received by the community or group it was intended to target. The message could then be honed or sent through different more adapted means for the audience. Essentially letting the message sender influence a group without interacting directly with them, while still receiving feedback response.

Seeing how a message propagates can also be used to identify which hubs or communities are more influential than others, if information is more likely to originate from certain bubbles.

We can examine what are the criteria of these messages originating from the influential communities. For example, some studies have noticed that more fringe and extreme communities can influence other ecosystems on the internet. The flow of ideas between these interconnected networks is likely why the mainstream media now gets some of their news from social media.

Indirectly, the collection of information and the visualization of silos can be used to categorized people belonging to them. We could attribute certain characteristics and qualities to persons frequenting a group.

Epidemiological model such as the SIR spread model can be used to see the propagation of messages through time and space. Similarly, percolation models can be used to see which variety of information can reach a tipping point and spread virally: its qualitative attributes or the ones of the network it's spreading on.

Another information we can get is whether applying different reproductive strategies for messages work better. Answering questions such as: Does quality or quantity matters? Which works best an R vs K selection strategies? What makes a message good, is it the high-volume, frequent repetition or high quality and low-volume?

Some studies have shown that on the internet it's a game of volume and brute force and not specifically intent and design to be able to reach a large audience.

Theoretically, all this data can be used to see trends, the spirit of the time, the zeitgeist. Having insights into the architecture and dynamics of the networks and the information that lives on them open many possibilities. The related field of big data, consisting of extracting value out of a humongous amount of data, is booming.

Unfortunately, as with anything on the internet, a considerable quantity of the data generated doesn't come from real humans but from algorithms. Studies approximate that 40% of the internet consists of non-human users. Consequently, the visualization of flow, the insights, the models, and the refining of messages are partly based on information given by bots.

Thus, a company's decisions based on such data might be indirectly based on the will of algorithms, hence leading them to deceitful conclusions.

Furthermore, the knowledge and visualization of the flow of information can be abused by actors wanting to spread a narrative.

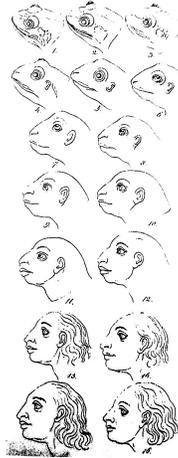
For instance, they might rely on side channels such as citizen journalists and fake news portals to then have their message be regurgitated by mainstream media. Effectively, they would have traded up the chain by using their insight of the connection between different networks.

Lastly, there are still questions regarding personal data and data gathering in general. Who is responsible when there is a breach? What type of processing is allowed on the data? Is the data subject allowed to update or correct their data? Who is the actual owner of the data? Can the data be transferred freely without authorization from the data subject?

These are all important questions we'll tackle in the last part when we'll discuss the solutions to the issues brought by the internet.

This concludes our review of what personal data is and how data on the internet is collected to be used in models. We've first seen what personal data consists of. Then we've looked at all the places personal data is generated and collected. We've seen the normalization of this process in societies. Later, we've examined how this data is useful for marketers, and how it creates a lucrative business to gather the data to resell it to them. Next we've pondered about different types of models and ways to use the data apart from direct marketing. And lastly, we've considered how this model could lead to misleading insights if it is based on algorithms and not human behaviors.

## Memes and Cults



J.C. Lavater, Physiognomik, Vienna, 1829

- Defining Memes
- Internet Memes as a New Mode of Communication
- Memeplex — The Meme Ecosystems
- Effective Memes
- Memeoids
- Relation to Cults

In this last section of our first part about artifacts and places, we'll explore memes, internet memes, and cults, their definitions, how they have transformed and crisscrossed, their relationship, their role as communication vectors, and the extreme forms that they can take.

Meme is a word that comes up in many conversations. It can refer to two related definitions, the classic one and the internet-related one.

Let's start with the classic definition.

The Oxford English Dictionary defines a meme as *“an element of culture that may be considered to be passed on by non-genetic means, especially imitation”*.

Keith Henson defines memes as *“replicating information patterns: ways to do things, learned elements of culture, beliefs or ideas.”*

A meme is a unit of culture, it is copied from other individuals, and propagates by being actively shared. It encompasses constituents of culture within itself. A mix of narrative, ideas, behaviors, and tropes.

The meme information has not only to propagate but also to have an impact and persist.

The memotype, the actual information-content of a meme, its semantic core, can have direct or indirect meaning. It can use figurative language that resonates within a culture such as commonly recurring images, rhetorics, motifs, and clichés.

In its physical form, its appearance, a meme can be contained in any media shell: verbal, visual, textual, auditory, gustatory, sensory, or anything the senses can allow.

These definitions are enticing but don't include the essential novelty that the concept of meme has brought: a parallel with genes. The name comes from a mix of gene and mimetes, from the Greek mimetes, the imitator or pretender. It was initially supposed to be called Mimeme but got abbreviated to meme. Thus, memes also add the notion that the transmitted information is granular and can be studied from an evolutionary standpoint. Memes are transported in their media package, the copies are subject to variation, and they compete for space in our memories and for the chance to be copied again. Only successful variants can survive.

Susan Blackmore re-stated the definition of memes as: *“whatever is copied from one person to another person, whether habits, skills, songs, stories, or any other kind of information. Memes, like genes, are replicators in the sense as defined by Dawkins.”*

Memetics is the study of the analogy between the elements moving in an “information society” and Darwinian evolution. This is done in multiple ways, one of them is to apply models to visualize the transfer of information, to see the criteria that makes them stick, to analyze what makes them successful and reproduce. We've done a great overview in the previous sections on big data and models of information flow.

There are two movements that argue different definitions of what memes are.

1. A unit of cultural transmission (that can be copied, located in the brain). That can be described as a memory item, a portion of neurally-stored information that is instantiated/caused by interacting with another person's nervous system. (I know this is heavy).
2. Observable cultural artifacts and behavior.

Some people think memes have a physical nature in the brain and others think that they only exist within society and not as observable entities in the brain. Essentially, one group defines memes as internal and another defines them as external to oneself.

The first group argues that in the future we could obtain technologies that would allow us to find such observable meme.

Due to these separate definitions, it's better to differentiate and study memes using two words.

- i-meme, for the internal cognitive phenomena like neuronal behavior, studied via fMRI, neuroimaging techniques, genetic profiling, hormonal tests, and neurochemical reactions.

- e-meme, for the external phenomena like culture and behavior studied by simulated propagation on social networks, game theory, attention and awareness studies, motivations, emotions, etc..

Like any scientific endeavor, it's important that things be quantifiable and well-defined, otherwise it's a show-stopper. Research on memes always precisely do that, for example let's quote a paper: *"A meme is information (using Shannon's definition as that which reduces uncertainty) transmitted by one or more primary sources to recipients who, as secondary sources, retransmit the information to at least an order of magnitude more recipients than primary sources, where propagation or the information persist at least ten hours and the information has observable impact in addition to its transmission."*

Most research focus on e-memes.

It's also good to be aware that there are skeptics about the terminology used when comparing memes to genes as they don't equate to one another. The critics call memetics a pseudoscience because memes do not follow the same selection criteria as genes. Namely, the definition of a meme is still vague, there is no scientific demonstration of the replication happening, the encoding of a meme isn't known, and the mechanisms of replication aren't stable.

Memes can thus be placed in between the science fiction ideas of brainwashing, viral marketing, and Darwinian evolution.

Regardless, playing with the notion that cultural information moves like genes is interesting in and of itself as a tool for thoughts.

In common parlance when someone says meme they can mean "internet meme," usually a photograph with a clever caption that is shared around the Web. Often created anonymously, remixed endlessly, and shared constantly, the most viral memes seem to materialize out of nowhere.

The term has seen a rebirth with the internet, even the Merriam-Webster notes that a meme is now popularly defined as *"an amusing or interesting item or genre of items that is spread widely online especially through social media."*

Limor Shifman characterizes these internet memes as:

- A group of digital items sharing common characteristics of content, form, and/or stance, which
- were created with awareness of each other, and
- were circulated, imitated, and/or transformed via the Internet by many users.

The author of the original meme idea, Dawkins, noted in 2013 that it *"has itself mutated and evolved in a new direction. An internet meme is a hijacking of the original idea. Instead of mutating by random chance, before spreading by a form of Darwinian selection, internet memes are altered deliberately by human creativity. In the hijacked version, mutations are designed — not random — with the full knowledge of the person doing the mutating"*

However, even though internet memes are associated with creative medium like funny image macros, this perception is limiting. Internet memes are "culturally

resonant items easily shared and spread online”, and as with anything on this communication channel they have to follow its rules to succeed.

As a consequence, the sharing and virality aspects are self-explanatory, these criteria are required of social media messages for them to pierce through bubbles. In that case, it isn’t surprising that the concept of memes, when applied to the internet, will have to be deliberately designed using attention grabbers such as visual content. In that sense, internet memes are only instances of memes and not a brand-new definition.

However, unlike generic memes, the appearance of internet memes is limited to what can be transported on the internet. This can be textual, audio, or visual.

- Verbal media memes: slogans, words, text, keywords, hashtags, etc..
- Audio media memes: songs, melodies, etc..
- Visual media memes: images, posters, “Photoshoped” pictures, caricatures, etc..
- Hybrid/audiovisual media memes: video, vines, etc..

Internet memes are culturally relevant, broadly resonant, organically developed, and voluntarily spread.

On the internet they have become a new shared cultural language, a way to convey meaning. It’s a new type of vehicle for communication, packing ideas into transportable containers that can evoke meaning, emotions, memories and more.

The sentence “a picture is worth a thousand words” applies well to internet memes.

Memes are convenient and accessible mental model creators. They offer a quick way to construct a mental representation of a situation, event, or object and allow to process, organize, comprehend, explain, judge, and formulate predictions and inferences about these former.

They provide a narrative in a condensed package, and so are tools for analysis. They are media rhetoric, deconstructing complex ideas using compressed symbolic images/text/audio.

As you can see, it makes memes excellent persuasion and propaganda anchors and hooks, you can revisit the section on propaganda and persuasion for more info.

Even if some memes weren’t created with a purpose, they will sooner or later be appropriated by political or business elites for leverage. Many memes, because of their symbiosis with social media, have to frequently show strong emotions that is with or against ideologies, show humor, parody, be snarky, silly, witty, angry, and most predominantly be poignant.

As was said in the social media section, it is our own confused cultural codes that are abused to make messages spread. That is why successful memes take stances, either as meme-aggressor — discrediting an idea, political program, politics, or media person or authority — or as meme-protector — a message to keep the status quo, enhance a person’s profile or authority, or protect a state ideology.

Memes frame the attention on a single aspect of an issue and cannot confer enough nuances due to their condensed form. They are filtered views of the world.

However, in the eye of the average person, internet memes are looked at as entertainment content, more precisely infotainment — like anything that is on social media. It is easy to overlook their power as they do not appear to have substantive content and can take the form of hastily constructed cartoons. Nevertheless, after the 2016 USA elections, the media outlets of the world started crowning memes as “*the new king of political communications*”.

Unlike TV, printed media, and most other forms of communication, internet memes are built for speedy consumption on smartphones and are prioritized because of the visual aspect of social networking. They provide a quick emotional hit in comparison with long-winded articles, and thus an instant payoff.

Studies have shown that people perceive internet memes via a peripheral route in their brain, according to Richard Petty’s {Petty, Richard} elaboration likelihood model of persuasion (ELM). This means that they rely on a general impression, the mood, and early part of the message contained in the meme and not on any significant cognitive efforts.

This goes together with the notion that internet memes are perceived as infotainment.

This peripheral route isn’t effective when it comes to long-term changes in attitudes but can have some influence on the short-term. However, as you can imagine, this can be countered with repetition, more units of the same message.

More than anything, memes are a way for individuals to express themselves, to show who they are and what they believe in. Consuming and sharing memes is an act of identification.

It has been found that there is a close relation between belonging to a subculture or having affinity to a group and the propagation of related internet memes. They are used as a form of commentary, or even rebellion against or for official discourse.

People might even seek out memes as a type of emotional release.

This creates a constellation of memes, a meme pool. In it, there are organizations of large groups that are copied and passed together, co-adapted for their survival. We call them meme complexes, or memeplexes.

The memes are aware of each others, like cross-breeding, sometimes cross-referencing the format, appearance, message, or semantic core of other memes. This symbiosis reinforces individual memes.

The memeplex, like an ecosystem, balances itself with different memes, creating a memetic equilibrium. Similar to how propaganda sells a coherent world of cohesive meaning. Some people like to talk of memes as the new urban legends medium, the modern hermetism or mysticism, others as an ecological forest. Experts in the domain of semiotic are getting interested in memes for this reason. Semiotic being the study of signs and symbols with an emphasis on their interpretation, context, and meaning. It covers many of the things

we've seen and we'll see, such as: ideologies, persistent beliefs, commonly held views, cultural anxieties, dominant mindsets, received wisdoms, expectations, preconceived notions, assumptions, widespread preoccupations, historical facts, principles, ideals, supposed eternal truths, unspoken tensions, shared hopes, master narratives, public opinions, prevalent attitudes, considerations of what is normal, outlook, established power structures, and more.

Through different means, such as the gathering of big data, it is possible to track the propagation of the memes across multiple communities and measure their influence, discover who influences others the most and which variants are best.

A research analyzing memes generation on online platforms has showed that fringe communities such as 4chan and reddit r/The\_Donald (defunct) were big generators of memes, which then were influential on more frequented social networks such as Twitter. Their messages were mainly political ones, imbued with emotional and hateful content.

Nothing surprising here either.

Even though we can track the spread of memes, the real origin of them is often unknown. Some have come to call this phenomenon crowd-sourced democratic expression, and others an intellectual apocalypse. That reminds us of what social media are about.

This means that there is no accountability for the creation of the message. It makes it harder for political groups to blame or retaliate against the memotype, or even criticise the creator, as they could with mainstream media reporters or journalists.

Indirectly, that's also an advantage for the propagandist, they can use memes as tools of black propaganda, hiding their identity.

We've seen that emotions and shock-value make a meme spread. What other criteria make a meme successful?

Let's state something from the get go: Memes do not have to be true to replicate. Memes aren't about their creation but about their spreading. The constant production of new content leads to a fight for the survival of the fittest.

Like genes, meme survival is measured along 3 axis fecundity, fidelity, and longevity. They also spread like viruses. There are studies quantifying the analogy with evolutionary pressure, showing the selection process and the movement between different communities, moving from fringe ones to more mainstream ones. Prosperous memes have to bridge cultures to live on. Being restricted to silos is a disadvantage and can lead to extinction.

Other studies show how the SIR (Susceptible - Infected - Resistant) model of disease applies perfectly to memes. Susceptible people being the ones who hadn't seen the meme, infected people those who were actively interested in its content and to spread it further, and the recovered were those who had seen the meme and lost interest.

These research and models confirm that memes can be studied like infections.

Consequently, they can be treated or have their propagation hindered by quarantine for example.

This is a topic that the author of the concept of memes, Richard Dawkins, directly tackles in the essay entitled “Viruses of the Mind”. Though the essay dives into the parallel with religious doctrines, it still puts down criteria that viruses have to fulfill to survive:

- Spread silently, be difficult to detect (by its host)
- Not spread if the virus is already present in the host (double infection)
- Not kill its host, or infer too much damage, at least not rapidly enough to stop the spread

The essay then extracts and applies this to memes with two conditions:

- A readiness to replicate information accurately, perhaps with some mistakes that are subsequently reproduced accurately.
- A readiness to obey instructions encoded in the information, so replicated.

When it comes to the shell of the message, the visual nature of internet memes adds to their potential persuasive power on social media, making them more attractive. They are comparable to editorial cartoons in newspapers.

An image has the advantage of stickiness and brevity, communicating concepts quickly. This is something that has been studied. Our brain interprets images faster than text, thus reducing the likelihood of thinking deeply about the content, as we said earlier. 70% of our neurons are in our eyes, and we process images 60 thousand times faster than any other media type.

Rational discussion is less effective than a visual campaign. Images are more emotionally evocative, and emotional cues have a preferential path in the brain. We do not even need to be aware that these emotions are elicited, they could be subliminal.

As far as metrics go, research in the field of marketing clearly show that visual content is more shared than anything else, help retain information, and make following instructions easier.

When it comes to the memotype, the semantic core of the message, we’ve already mentioned that successful memes are reflections of us. It is worth reiterating. A meme is an expression of our culture, our beliefs, behaviors, and values. The ones that go viral are unleashing our repressed cultural agenda, they don’t use novelty but use a potential that was already there. They exploit our latent, yet intrinsic, gaps in our cultural code, using our cultural vulnerabilities, the ones we aren’t immune to. Therefore, memes don’t compete for dominance by appealing to our intellect, our compassion, or anything related, but they compete on triggering our automatic impulses.

Logic and truth have nothing to do with memes, but they rely on our flight-or-flight reactions, the fastest reactions. From that perspective, memes aren’t really pro-social but anti-social.

Like viruses, memes reveal less about themselves than about their hosts. We wouldn’t be sick if we had an immune system capable of recognizing the shell

and then neutralizing the code it contains.

Thus, memetic material that is provocative, sensational, making news headlines, and shocking will be more successful. Studies show that people are more willing to share memes that evoke stronger disgusts (Heath et al.).

Another study conducted in 2017 related to an analysis of the keywords used in memes shows that the most popular memes were politically related. From USA MAGA movement, to the USA libertarian, to the president of the USA at the time (This study was USA-centric).

That means the content often acts like a propaganda anchor or hook, and is receptive to the current paradigms and belief systems.

Then this all manifests through real consequences such as media confusions, lack of trusts, protests on the streets. It's all viral memetics in action. We'll dive into consequences in another part.

Another criteria that helps survival is whether a meme can create a symbiotic relationship with other memes, what we referred to as memeplex. The meme could already fit properly with others, cooperating, or it could develop progressively a real or artificial compatibility.

Ganging up helps the meme flourish, and the longer they are attached together, the more they'll merge into a single package, a co-evolution.

Additionally, memes can have defensive systems, reject other memes that would hurt it. Consequently, creating an intolerance within the meme complex.

The content and the medium aren't sufficient alone, the context is extremely important too. We need to take into account the external factors such as:

- The timing to coincide with major events
- The architecture and dynamics of the network
- The media literacy and facility of the target population

Let's now review some of the results of research related to meme success.

The University of Memphis research shows that for an image macro to be successful the predictor variables were:

- A shorter memes (fewer than four words)
- The use of concrete terms (more memorable than abstract language)
- Avoiding swear words as they hamper virality (negatively correlated)

A research on military memetics by Dr. Robert Finkelstein digs into the measurement of the fitness of memes. It calculates the memetic fitness unit as the number of person-hours transformed. The most fit memes correlated with:

- Propagation (.428): number of recipients, type of recipients, dispersion of recipients
- Persistence (.284): duration of transmission, duration of memory
- Entropy (.087): small, medium, large (At this time, we consider smaller memes to be more important than larger memes. Larger memes may all

be memplexes (e.g., the typical human brain cannot hold more than 10 “chunks” of information in short-term memory))

- Impact (.20): Individual consequence, societal consequence

That means, according to this research, that the most important factor to fitness are propagation and persistence, and impact of a meme, but mostly propagation.

The research also summarizes some criteria that should be applied to the information content of the meme, such as:

- accuracy
- relevance
- timeliness
- usability
- completeness
- brevity
- security

The computer scientists at the Hebrew University tried to use an algorithm to predict the spread of certain hashtags on Twitter using a dataset of more than 400 million Tweets. Their findings were that successful memes factors were based on:

- The meme’s content
- The meme’s context
- The social graph

Another paper on the military application of memes proposes the following:

- Meme conciseness (1-10 words)
- Choosing information which propagates, has impact and persists (Info-PIP), and be able to monitor them via metrics

Some papers even go as far as to say that it’s not really about the meme criteria but the network criteria. That’s what the Indiana University’s Center for Complex Networks and Systems Research found: memes that went viral were no different from those that didn’t, the success was due to the structure of the social network.

These research all go in a direction that echoes what we said earlier: memes are a reflection of us. These memes do not necessarily have to be malicious, they could have beneficial purposes. Today memes have surpassed genes as the dominant driver in human behavior and we have to understand their importance. For that we have to develop a healthy cultural immune response to hostile ones. We should learn to quarantine, distance ourselves, and apply immune attacks to neutralize them when necessary.

These are requirements in an information society.

Two concepts come to mind in relation to our society: memocides — the deliberate eradication of a memplex from a population, by either killing the

host or by censorship — and eunemics — inspired by eugenics but applied to memes, deliberately improving the quality of the meme pool by selective breeding. Eunemics is done through memetic engineering, using engineering principles to mold them.

This means memes can also be informational weapons, propaganda tools.

When meme and memplex are brought to their extreme, a person is overtaken by them, letting go of their own survival instinct and favoring the meme instead. In the symbiotic relationship, the meme has won and consumed its host. The people affected by this phenomenon are called memeoid.

Examples of this include kamikazes, suicide bombers, cult members, and others. Keeping in mind that the previous criteria for reproduction still applies, namely that the meme should keep their host alive long enough to spread properly.

This is a trading between genetic reproductivity and memetic reproductivity, which might not coincide. Promoting the memplex might not be correlated with promoting a gene pools. Replacing the purpose of one's existence with the spread of the meme.

Richard Dawkins cites the following when it comes to memplex consuming individuals, it becomes a sort of narrative.

- Impelled by deep inner conviction that something is true/right/virtuous, against all reasons
- Make positive virtue out of the strong stance on the meme
- Conviction that mystery is a good thing
- intolerant behaviour towards perceived rivals of the meme
- If follow a different meme from parent it comes from a charismatic individual
- The internal sensations of the meme holder are similar to ones associated with sexual love

Strong memplex are thus similar to cults, people being mind controlled by ideologies and its members turning into puppets of the memes.

Singer's six conditions of mind control reverberate this idea:

- Keep the person unaware of what is going on, and what changes in themselves/their behavior is happening.
- Control the person's social and/or physical environment, especially the person's time. Remind them of the narrative all the time.
- Systematically create a sense of powerlessness in the person. Keep them away from their former social support group or identity.
- Manipulate a system of rewards, punishments, and experiences to inhibit the former identity. Accomplished through various methods of trance induction, speaking patterns, guided imagery, etc..
- Manipulate a system of rewards, punishments, and experiences to promote the group's ideology and behaviors. Compliance are rewarded while questioning or doubts are met with redressed and rejection.

- Put forth a closed system of logic and an authoritarian structure that doesn't permit feedback and refuses to be modified except by leadership.

These are all things that we've seen in the mix of social media space and the usage of memes in their memplex.

This is especially true of the attention-reward system of social media. As social primates, attention is a measure of status. When we get attention our brain releases chemicals such as dopamine and endorphins, creating an addiction (AAR: Action - Attention - Reward). This system can be shortcut with memes. The memplex, and the ones carrying it, requires intense social interactions and behaviors such as sharing the meme or reenacting its content.

The members then create their own isolated bubbles of coherent meaning. Some of them opposed, clashing, and creating the rise of many of the things we've seen so far.

Clearly, as with propaganda, children are more vulnerable to subversion and are easy pray for memplex. Children are pre-programmed to absorb useful information at thigh rate. It is harder as adults to remove the pernicious and damaging information that have been introduced early.

Deprogramming studies, used to get people out of cults, can be applied to memeoids too. They rely on invoking new capture-bonding social reorientation mechanisms.

Similar to our conclusion on propaganda, we have to say that some memplex can be considered pathogenic but others can be beneficial or relatively harmless. The judgement is subjective.

In a strict sense, everyone, including you and I, are memeoids, carriers of memplexes. We are all hosts, one way or another, but not everyone reaches a degenerative state, even though we have the potential.

A skill that should be developed is metamemetic thinking: being able to recognize and acknowledge the content of memplexes, the illogicality in them, and anything related to their attributes.

The metamemetic can also be used to understand the people associated with them. Coming back to our data and metadata section, memes are information and thus can be used to characterize, analyze, and classify people.

This concludes our review of what memes are and their relation with the internet. We've first seen their definitions, one is based on a comparison with genes applied to cultural information, and the other to internet image macros and tropes. We've then made the parallel to how these two aren't dissimilar and how internet memes are only instances of memes adapted to social media. We've taken a look at how people perceive these memes, how they are used as a way to communicate and express one's identity. Then we've dived into the memplex, how memes associate themselves to create a world, to better survive. Next, we've inspected what makes some memplex successful by summarizing some research. Finally, we've investigated the close relation between the extreme form that memplex can take, turning people into memoids, and cults.

## **The Actors and Incentives**

## New Economies: Information Economy, Attention Economy, Data Economy, Surveillance Economy



E. Sibley, *A Key to Magic & the Occult Sciences*, c. 1800

- Data and Attention as New Assets
- How Much Value
- The Actors (Social Media, Ads Networks)
- What They'd Do to Get It
- What They'd Do to Protect It

The artifacts we've previously seen have given rise to new types of economies, tools, and arsenals that can be used by different actors for different incentives. Let's start by focusing on the economic aspects by looking at actors such as social media platforms, newspapers, and advertisement companies.

Life in an information society is about moving data, the new raw material, around our manufacturing pipelines. This data is then consumed by either paying with attention or money.

Data and attention are the two assets of the digital economies that emerged.

Whoever holds the means of productions, by centralizing and monopolizing them, has a tremendous advantage in any economy. In a data economy these are the data brokers who figuratively data mine the raw material, store it, and keep it well guarded — as is required in any intangible economy to succeed (See *Capitalism Without Capital: The Rise of the Intangible Economy*).

The other new asset is attention. In an environment where it is at the same time so hard to reach an audience and, once reaching a threshold, so easy to spread virally, having the skills to capture attention is valuable. This is due to multiple factors such as the rise of social media, the average users becoming generator of content, and the ever-growing infobesity.

Davenport & Beck (2001) define attention as *"focused mental engagement on a particular item of information. Items come into our awareness, we attend to a particular item, and then we decide whether to act.*

Its scarcity turns it into a prized resource, constructing an attention economy. Attention is exchanged as a commodity, either by giving it or taking it — an intangible good on one side, money and physical goods on the other.

There is a fight for this resource, the corporate entities need it because the digital economy is in sync with advertising. The drivers and generators of money are buyers of attention and data, namely marketers and advertisers. Just like traditional media advertising, the online world follows a model that uses a linear process called AIDA: Attention, Interest, Desire, and Action. Hence, social media platforms, online newspapers, and others make money by selling ad spaces, selling targeting information using the data gathered, and giving access to or selling the data itself.

Marketers have two choices when it comes to social media: either passive marketing — gathering data from their consumers posts and public information — or active — engaging with users, creating polls, paying influencers to advertise a product, etc..

Both parts are facilitated by platforms that allow tracking and analyzing the results of their campaigns. Advertisement is only a sub-section of marketing.

As for online newspapers, and many others, they have chosen to either sell ad space, thus attention, or switched to a subscription model in which the customer pays to get access.

Some argue that the centralization of ad services forces companies to offer paid services, leading to an overall more expensive online experience. There are big questions regarding the value of the content we consume online and how much should be paid for it. The concept of micro-transactions and micro-payments comes to mind, we'll come back to them in the solutions part.

The internet conundrum is that users have developed a habit of expecting online services to be free. So, to make the services offered profitable, the owners have to extract valuable things from their users, namely their attention and generated data.

The digital culture expert Kevin Kelly describes the expected attributes of this economic space as:

- Immediacy - priority access, immediate delivery
- Personalization - tailored just for you
- Interpretation - support and guidance
- Authenticity - how can you be sure it is the real thing?

- Accessibility - wherever, whenever
- Embodiment - books, live music
- Patronage - “paying simply because it feels good”,
- Findability - “When there are millions of books, millions of songs, millions of films, millions of applications, millions of everything requesting our attention — and most of it free — being found is valuable.”

In direct relation with the data economy, a sub-type of economy has appeared that specializes in a particularly profitable data type: personal data. The surveillance economy, as it came to be called, centers itself around making profit from gathering personal information, commodifying it.

This data is obviously more valuable and can be sold for reasons other than precise targeted marketing, such as creating a voters profiles database to be sold to state actors. This was the case of Cambridge Analytica, who used Facebook as a tool to gather information. Allowing them to join up to 7 thousand data points on 240M people. We’ll see more of that later.

This grants companies access to information that can be used to tailor their products to their customers’ needs, and customize their marketing campaigns to specific categories of people, to what we call “buyer personas”. This is good for passive marketing.

For example, a job ad can be sent precisely to men between 25 and 36 that are single and have interests in cars.

When so many data points are involved in identifying an audience, this is referred to as microtargeting.

In the past, advertising was used with the goal to inform consumer choices, today it is predominantly used to persuade them, going back to our section on persuasion and propaganda. It steers consumers toward the brands which invest more in advertising, rather than those that are sustainable and responsible but less competitive. Thus, driving global consumption artificially.

Active marketing, engaging with users, works well in a surveillance economy too. Companies can perform direct continual experiments on their customers without them being aware of it nor giving consent.

An A/B or Wizard of Oz testing phase that would’ve taken months to perform can be done in a matter of hours on social media, an almost instantaneous feedback.

In the past, marketing used to be more of a one-to-many type of communication, with the internet it now appears more intimate, a one-to-one customized experience with the brand. The company can build a relationship with their customers for long-term success.

This relationship can then work in their favor through the viral nature of social media. The consumers who find what they are looking for will share their positive experience, while those who didn’t will also communicate it. The opinions will proliferate and increase in number.

From the data gathering side of the equation, big tech companies are then

justified in amassing data at all costs, tracking and analyzing. This affects privacy and control over our lives, we'll see some of the deleterious consequences later. The data includes location history, preferences, age, name, and other things we've seen in the previous data and metadata section.

These three or four types of economies, digital, data, attention, and surveillance, clash together. The first one generates a mountain of advertisements and content that floods people, making them more picky about what they pay attention to. Accordingly, the value of attention rises, it being more scarce, creating additional incentives to invest into specific targeted advertisement, hence more surveillance.

A true arms race driven by a contamination of the supply that is often filled with irrelevant, redundant, unsolicited, low-value information. An adverse effect of this information revolution.

One of the many consequences, which we'll see later, is something called continuous partial attention, a phenomenon where someone's attention is constantly divided. It can lead to increase stress and an inability to reflect or make thoughtful decisions, sometimes related to analysis paralysis.

This consequence is convenient to some actors, especially in relation to what we've seen in the propaganda and persuasion section.

There's a lot of money involved and many reasons to secure a position in these new economies. As with any new commodity that spawns, is lucrative, and fast growing, it attracts regulators and policymakers that want to restrain its control and flow.

Every year, companies worldwide spend more than 1.3 trillion dollars on commercial communication and 600 billion dollars on advertising. The titans of the internet, Alphabet, Amazon, Apple, Facebook and Microsoft look unstoppable. They are part of the most valuable listed firms in the world. Their profits keep surging: they collectively racked up over 25 billion dollars in net profit in the first quarter of 2017.

This is compounded with the feedback effect that more data encourages more data. This confers an enormous advantage to already large incumbents, the ad technology suppliers that have amassed a wall of well guarded data.

In this economy it is quantity over quality.

The giants span different fields, Google can see what people search for, Facebook what they share, Amazon what they buy. There's no room for small players such as online newspapers, or any other SMEs, they can't compete. This means the biggest players have a strong grip on the supply chain, both the data, attention, and the ad tech.

Size isn't the issue here but the danger it can have on the consumers in these economies. It impacts everyone along the supply chain, from publishers, to advertisers buying ads, and the consumers.

This can create conflicts of interests, giving a self-preferenciation to specific suppliers of ad technology. These later can then control the price of access to

it, its quality of service, and the transparency going along with it.

With such control, these companies can thwart competitors, either by hoarding more data and making it impossible for others to rival them, or by acquiring or destroying contenders.

For instance, many think that Facebook's acquisition of WhatsApp for \$22 billion falls in that category, namely creating a barrier of entry and stifling competition.

Unquestionably, these data brokers are nothing without their network of buyers, the advertising companies and other entities interested in getting access to mined data and attention. While there are many small players, the bigger ones will often sign partnership deals with the data brokers, so-called third-party partnership (or sub-contractors), to exchange and interoperate data laterally. There are countless examples of these generally non-transparent deals, at least non-transparent with regard to the data subjects which have their information exchanged without their consent.

For example, AT&T may use third-party data to categorize subscribers without using their real names to show them ads. In practice, that means AT&T can find out which subscribers have which health issues — or which ones bought over-the-counter drugs to treat it. The companies extracted this kind of information from the databases accessed through third parties which contained subscribers' spending.

An investigation by the New York Times from 2018 detailed how Facebook had made special agreements to share/give access to personal user information and private chats to 150 tech firms, including Amazon, Apple, Microsoft, Netflix, Spotify, and Yandex. The list also included online retailers, car-makers, banks, phone manufacturers, and media organizations.

Facebook distinguished between two types of relationships: integration and instant personalization partnerships.

The first one is about offering Facebook's features outside its own app or website, the users having to sign in to their account to allow it.

The second one, "instant personalization", is about allowing other apps to interact with Facebook private messages to customize them.

Facebook noted that it ended "nearly all" of the integration partnership and most of its personalization partnerships.

Facebook is a gargantuan player, but only one among many like Google and Twitter. They all have such deals and act as data brokers.

The most interesting type of partnership relying on these gigantic databases of personal information are the ones with state actors. For now, let's only note that the USA government requires would-be immigrants and visa applicants to submit five years of social media handles for specific platforms identified by them, mainly Facebook. We'll see how lucrative social media are for states later.

With lots of money and people involved, many aggressive tactics are used to

get the attention and personal data of people, any legal means are allowed. That is why they rely on persuasive technology, a term used to refer to any technology designed to change attitudes or behaviors through persuasion and social influence. In our case, they are used to persuade to act based on ads, pay attention, and give personal data.

The use of persuasive design is custom-fit to the receiver, for example it can be based on age-appropriate desires.

The preliminary information can be gathered from all the sources we mentioned in our data and metadata section such as smart utilities, and our daily ubiquitous online activities. This is all possible because the user inadvertently agreed to a hidden privacy policy, in most cases without reading it. In so far as this is the argument used by these platforms to allow this, while making it as cumbersome as possible to understand what the policies imply.

Then, once the target is set, the software platform algorithms will explicitly or implicitly attempt to win the attention of the users through interface and psychological tricks based on the interests and personalizations from the data extracted earlier.

This includes mundane things such as catchy click-bait titles of news articles, and visual tricks such as using shocking pictures, impactful fonts, and attractive colors. The usual in marketing and other types of media (TV, newspapers, radio).

The new nefarious techniques rely on dark patterns, user interfaces that are designed to mislead and direct users into acting a certain way. This includes hiding parts of the interface that are supposed to be there for legal reasons, encouraging users to sign up or buy services or items they didn't intend to, and more

Additionally, the platforms will create an environment that nurtures attention, shaping it using the data acquired. This ranges from benign things such as showing users what they are looking for, to turning the digital environment into a casino-like environment.

Social media are especially known to employ this stratagem, relying on the craving for social feedback that people want and mixing it with a reward system, be it "like", "views", or "shares". Overall, this is a vicious cycle made up of a classical conditioning scheme that creates a drug-like addiction for the users participating on social media.

These techniques work well on adults but even better on kids. Perniciously, the different platforms involved have used them to target younger and younger people. The typical age when kids get their first smartphone has fallen to 10yo. There's more profit to be made out of a blank mind than an already filled one. This manipulation for profit is a reminder of our section on propaganda and how having full control of an environment allows for indoctrination.

The children are then caught in a virtual environment replacing their real-world needs and basic human drives: to be social and obtain goals.

To reiterate clichés, for teenage girls it could be wanting to be socially successful,

and for teenage boys to want to earn competences. Meanwhile, they can easily fall victim to the internet's attention and surveillance economies — an endless pursuit of stimulating virtual points which they believe will make them happy and successful.

I digress, we'll have a full part with consequences.

Strikingly, the tracking and fight for attention starts earlier than childhood, the digitalization of our lives starts before birth. This is why data on pregnant women is the most valuable. We are the very first generation to be datafied before birth, this is a historical transformation.

On social networks, people most of the time want to entertain themselves, and entertainment is what makes them stay. One type of very popular entertainment is political infotainment, a sort of caricature of politics. A large portion of end users visit social media only for politics, and so the platforms will be incentivized in promoting this type of content. They give what people are looking for.

Many of these digital spaces rely on something called a “feed” or “home” page that will be generated and presented by default. This page will be optimized and curated by algorithms for the goal of the platforms. It is highly individualized, the news and information are selected by engagement value, intentionally designed to isolate end users from information that will make them leave, and creating a self-reinforcing feedback loop of confirmation, thus satisfaction.

From recommendation engines, search results, trends, autocomplete forms, it all happens through the mediation of algorithms. Whatever content is able to satisfy the criteria of the algorithms will be promoted, be it through clickbait titles, paying for fake views, fake reviews of products, bots interaction, and outrage-related and emotion inducing content.

The objective is to predict what we are more likely to interact with: click, view, engage.

The algorithms themselves are impartial, they do not know what the actual content is, and cannot discern between what is true and what isn't. They are simply good at what they were programmed to do.

The algorithms are trade secrets of the platforms, opaque tools that influences millions of people each day. The data brokers and networks use this as a justification of non-accountability for the consequences, something we call mathwashing. Hiding behind the algorithm and pleading free speech.

Algorithm amplification is the phenomenon we are experiencing, the automatic radicalization of views and disinformation as an instrument for more views and spiraling out of control. It is a business choice made in pursuit of profit.

Social media will reward, through the point systems, extreme stances on subjects, these serve as the lubricant for these businesses, making them more profitable and influential. Studies have shown how users feel satisfied when finding a niche to cater to that generates a lot of these points (likes/shares).

This is an effect that is comparable with TV long-term media effects theory. It states that the more an individual watches television, the more they believe

social reality matches what they see on it.

These have ramification in the real world, the consequences can be dire, as we'll see later. For example, hate speech amplification can thrive and fuel genocide. Internet platforms play a dominant role in our conversation, extremism cultivated online has real world ramifications.

Evidently, they are now under public scrutiny and lawmakers want to intervene but social network, ad tech service providers, and others in the loop will fight to defend their castle of data.

The most common argument is that users have consented to what is happening by agreeing to the privacy policy and EULA they were presented with when signing up to the service. It is ok because it is the inevitable conclusion of our online activity. In other words, asking companies whose business models revolve around exploiting personal data for consumer-influence techniques to explain their privacy policies is like asking someone to shoot themselves in the foot.

The companies are now tweaking their tactics, using a patch-like approach rather than tackling the real issue, which is the core of their business. We'll see in the last part some real solutions.

For example, AT&T recently said they would stop sharing users' location details with data brokers, Facebook said it stopped allowing advertisers to use sensitive categories for targeting, Google said it's now allowing users to download masses of their data.

Recently Google is also going to remove third-party cookies, to then allow third-parties to have access to the data only through them and getting information about groups and not individuals. They also get information directly from other sources such as their analytics and AMP service. A sort of differential privacy. Arguably, these give Google even more power over this type of data and drives away competitors.

In some countries, like the USA, the companies hide behind laws related to free speech to justify their policies. They are claiming that they do not want to be arbiters of truth.

That helps in taking the blame away from them, leaving them unaccountable as no USA critics want any platform to act as a censor.

As a last resort, like in any industry big enough, these companies don't shy away from using their money to convince the lawmakers anywhere in the world. Between 2005 and 2018, the big five tech in the USA have spent more than half a billion dollars lobbying the USA Congress, and donating to parties. Literally purchasing power.

Moreover, other databrokers also spend as much, companies such as CoreLogic spent as much as \$215,000 on lobbying in 2020; and Acxiom, which spent \$360,000 on lobbying in 2020 for issues related to data security and privacy.

Amazon, Apple, Facebook, Google and Microsoft have collectively thrown \$582 million at legislators in an attempt to influence the

lawmaking process and make sure their voices (and interests) are taken into account.

All of the firms have taken a position on privacy policy, with the issue coming up 3,240 times in all reports files—by far the most talked about topic. Last year alone, \$66.4 million was spent on privacy issues by the tech giants. That includes \$16.6 million from Google, \$15.1 million from Amazon and \$13 million from Facebook.

Whatever legality they deal with, like anything legal, depends on the country where the law is applied. Thus, any solutions will be localized, as we'll see later.

This concludes our review of the emergence of new economies in the digital space with regards to social networks and ad tech providers. We've first seen the two new assets: data and attention. Then we've looked at their worth and which actors had incentives to capture them. Next, we've seen how a few are owning the pipeline in this new infrastructure and how they have agreements with third parties. After that we've dived into some of the manipulation tactics used to gain such assets. Finally, we've listed a few of the defenses some of these companies have used against policymakers.

## Internet, in Between the Corporate, Private, and Public Spheres



W. Blake, The Sun at its Eastern Gate, c 1815

- Availability of Information
- Networks and Cultures
- Individuation
- Self-Generated Societies
- Making Up Your Own Mind + Learning & Creativity
- Citizen Journalist
- Cognitive Effects
- Private Life Becoming Public Life
- Passion Economy
- Extreme Neoliberalisation

The internet is a new resource and when introduced in our social structures it has fueled the construction of utilities around it. Like any tool it has no effects on its own but only through its usages. In particular, it has altered our capacity of communication making it interactive, multimodal, asynchronous or synchronous, global or local, many-to-many, one-to-many, one-to-object, object-to-object.

In this section we'll go over some of the things the internet allows to do through the platforms and services hosted on it. We can't go over everything because that would be equivalent to describing what modern life is about. Instead, we'll

paint a rough picture of the internet in between the corporate, private, and public sphere.

We can describe ourselves as an information society, an internet-everywhere society. Calling ourselves digital natives, digital citizens, digital cosmopolitans, and netizens.

Everything that can be digitized gets digitized. According to a study published by Martin Hilbert in *Science* in 2011, 95% of all information in existence on the planet is already digitized and accessible through the internet.

This has shrunk the globe, brought knowledge to everyone, altered the way we communicate and connect, changed the way we make money, and changed the way we think.

The internet reflects us, it can convey the best and worst of humankind. It is an open-ended system, like our societies, with the inter-relations mapped in the digital space, with all the same logics that exist between cultures, organizations, and technologies.

Similarly, the internet is networked and so are our societies: constructed around personal and organizational networks, without clear boundaries. Thus, the same paradigms and dynamics that apply in our real world are echoed online. Studying the internet is studying anthropology.

Previously we've seen how this bridging of cultures online makes us shift from high-context cultures to low-context ones, or informational ones. Because of this, we are forced to learn to communicate in a different way, with an emphasis on collaboration, learning to negotiate, to accept disagreement as normal.

Paradoxically, this has made us more socially conscious, and social in general, on the internet than in the physical world. There is less distance, it feels like the globe has shrunk, and that has intensified social interactions, for better or worse.

Some studies have observed that overall, there is a correlation between sociability and internet usage. This applies to civic engagements and other types of relationships. This is a new kind of sociability, one that is driven by permanent connectivity, especially on social media.

When bridging cultures a common language has to be chosen, and on the internet it is often English that dominates. It composes around 30% of the internet according to estimates, but isn't the native tongue of most users. This can limit the spread of information from one cluster to another, create boundaries for communities, an inequality of information, an inequality of representation, and shape the digital experience and views of people on the internet. The language, and indirectly culture, barriers can direct the flow of information, tending in the direction where it is sometimes more domestic. We'll get back to this in the consequences part.

The apparent reduction in distance also creates networking opportunities. In the past, interactions were limited to the personal networks; people being favored for whether they went to a prestigious school, university, or worked at a well-known company. These days we can be exposed to a diverse range of networks that

are much more accessible, increasing the employment prospect.

This applies to creativity too, being exposed to so many diverse ideas, different ways to see a problem. Creativity is an import-export business. Taking things that are ordinary from multiple places and putting them in totally different settings. What is called cognitive diversity.

Additionally, widespread connectivity brings the possibility of working from almost anywhere in the world, at any time of the day, if the job doesn't require to be on-place — that is if it is an information related job. This unlocks tremendous freedom and autonomy.

The concept of autonomy is an important one, as it relates to another one: individuation. When moving from high-context society to low-context information society, the process of individuation takes place. Some ironically calls it the “*ME-centered*” society, or the “*selfie generation*”. This isn't something new, it's been happening for a couple of years, but it is more widely spread and the internet is a catalyst.

Concretely, this translates into the decline of the definition of the self based on organizations and organizational roles, such as work, nation, and family. The individual is now in the center and doesn't find meaning in these classical system, sometimes leading to a cross culture frustration.

Nevertheless, this is not the end of the concept of community but the end of having it based on places of interactions. Instead, it has shifted toward the self-authorship of the community, one based on personal ties, social relationships, individual interests, values, and projects. As a matter of fact, the individual is not isolated, nor less sociable, but redefined as a networked individual with a quest for like-minded people.

The information society is a network of self-authored individuals.

The transformation and evolution in culture bring with them a reorganization of economic, communication, and political activities. According to some research, it is correlated with a sense of empowerment, increased feelings of security, personal freedom, and influence — all in relation with overall happiness and well-being.

Whole communities join together and participate in their own identity development, as a choice. In this model, people replace blind reverence for authority with authenticity.

In the past, information were shaped and based on hype, now people crave what is genuine and transparent. This is a change in perception with a focus on raw emotions and connections.

This authenticity is an essential aspect for identity development, it is how we identify ourselves and create our stories. Our narratives are based on our interactions in this participatory network. We are the creators, refining our persona with the help of the individuals that surround us, to whom we tell our story.

McAdams (1993) asserts, “*Once an individual realizes that he or she is responsible for defining the self, the issue of self definition remains a preoccupation*”

*through most of the adult years”.*

Being the subject, the individual, in the process of creation is what is meant by autonomy. This is accompanied by an urge to not submit to institutions, especially for minorities. This switch in mindset is highly correlated with social autonomy, independent-minded citizen able to participate in self-generated networks.

This autonomy materializes itself in society through entrepreneurship, creative works, proactive consumers, self-informed critical thinkers, pedagogical platforms that allow self-learning, e-governments, grassroots movements, etc..

The paper entitled “*The Social Media Mindset*” lists six major types of autonomy:

- Professional development
- Communicative autonomy
- Entrepreneurship
- Autonomy of the body
- Sociopolitical participation
- Personal, individual autonomy

More than anything, to be autonomous means mastering our tools, grasping how to make algorithms work for us. They are ubiquitous, we are surrounded by them, the internet is mediated by them. Hence, we need to muster their strength.

To be internet literate implies understanding the technology that drives it. The customization and recommendation engines can be used to facilitate our daily routine, letting the users create their own personal optimized environments.

Social networks are used to create our own constructed world, which includes everything from e-commerce, education, entertainment, to sociopolitical activism. The users group together according to their interests and tailor it to their needs. A self-constructed society with people yearning for honesty, genuineness, transparency, common interests, and connections.

Many of the real world has migrated to the internet, from web marketers, work organizations, service agencies, governments, and civil societies.

Technology, being material, is based on products made by people based on their ideas, values, and knowledge. We adapt the technology to fit us, rather than adopting it. It is built into our society and thus it has to follow its constraints. Obviously, social media platforms are trying to monetize the process, turning it into a business.

Collectively, this has brought us to an era of creativity. Where everything is a remix and shared. We aren't bound by the mainstream media gatekeepers like TV, radio, newspapers, and academia. Information is now freely available on the internet, accessible by anyone, from the worst atrocities to the most awe-inspiring instances of human kindness.

In the internet society we are forced to broaden our collective perspective, a perspective that is more global.

The informational freedom carries with it transformations in the sociopolitical realm. There's a widespread availability of tools for creating and distributing content across the globe. Most often, there is no need for training nor expertise to participate, everyone is empowered to mass media — A direct access to million of other people in an expanded community.

We bypass traditional media, letting us challenge the assertions of powerful corporations, government officials, news reports, and television advertisements. We do it through blogs, Twitter, Facebook, and others.

Everyone is an author and can express their thoughts to the world and this undoubtedly means that some people are going to spread disinformation, misinformation, and other types of erroneous information.

Our new distrust in authority and increasing doubts, can be abused through our cognitive biases. The attention economy, with the never ending competition between all actors, is filled with manipulation.

This is something the netizens are slowly learning. We'll come back to biases later.

The constant connectivity has given rise to a more democratic and participatory form of journalism: citizen journalists. The audience employs the press tools to inform one another. The public now plays the role of collecting, reporting, analyzing, and disseminating news and information.

There are upsides and downsides to this new development. As we said, these are amateurs, people without journalism training, and so the quality of the reports and coverage can vary, is subjective, heavily opinionated, unregulated, and can be abused by malicious actors — such as spin doctors.

However, it can also promote human rights and democratic values to have the people join together and collaborate in this endeavor.

Social network websites, accessible to everyone, have provided an alternative for activists to report on their activities. Social media also allow real time participation and messages can be sent quickly in reaction to events.

This is particularly helpful during an earthquake, street movements, and protests.

Lots of things are now shaped and decided on the internet, it is tightly linked to political changes in the process. Citizen journalists now surround all the protests and movements these days. These movements, rejecting authority, are often without leaders, more spontaneous, and full of emotional outbursts.

The media of choice to express feelings about a situation are internet memes. They act like the modern era version of caricatures found in traditional newspapers.

Some memes have been put forward in democratic campaigns such as sharing messages about climate change. Though arguably, the research hasn't found their impact in altering mindsets that impressive. In that study only 5% of participants changed their minds.

Memes, like caricatures, can also act as a power and counterpower, a battle of

communication. Humor has always been a tool for people to express feelings and thoughts that were repressed, to fight against oppression.

This is the case in countries where people have to bypass censorship and rhetoric by reusing the semantic meaning of the slogans, ideas, and terminology. They reuse the language, twist it, satire it, to reinterpret it in their own way. They use the official language in reverse by applying it with humor.

Still, we have to remember that citizen reporting is full of biases, doubts, lies, polarization, conspiracy theories, and subjectivities. These can also obviously be manipulated by other actors, as we said.

Similar to citizen journalists we are seeing the rise of citizen science, which we won't dive into here.

Let's now jump a bit into some of the effects that being constantly online can have on our cognitive abilities. In a place of never-ending multitasking, attention economy, infobesity, and new social concepts.

This will be reviewed again in the consequences part.

Our attention is now always divided between multiple media sources at the expense of sustained concentration. Everything tries to attract our attention in this hyperlinked addictive environment and we got used to it.

Education providers can already see the effects this has on children attention span: their attention is more shallow.

Studies show a significant effect on cognitive performance, where even short term engagement reduces attention scope for a sustained duration after coming offline.

Memory-wise, the vast array of information has changed the way we retrieve, store, and even value knowledge. The internet is now acting like a transactive memory, externalizing our thoughts — a helper, a memo, a memento.

We have most of the factual information in existence at our fingertips, introducing the possibility that the internet could ultimately negate or replace certain parts of our memory system, especially the semantic memory — memory of facts.

Multiple research show that people searching online were more likely to remember where they found the facts rather than the facts themselves. We are more reliant on the internet for information retrieval.

I've dived into this topic previously [here](#) and [here](#).

At the group level this can be efficient but at the individual level it can hinder how we recall the actual information. The internet sometimes even bypasses the ability to retain where we found the information when it gives us the opportunity to search for it. We don't have to remember the exact information anymore, nor where its located, just that it can be searched and that it'll be available.

This cognitive offloading using an external long term storage can be beneficial to focus, not on facts, but on aspects that are not retrievable like meta information, conclusions, and emergent hypothesis. It frees some space to think about other things than plain facts.

Though other research show that analytical thinkers are less likely to rely on

such means in their day-to-day than other people.

Cognitively, the internet also creates new ways to learn. Any new skills and information are available in this space. People now have more breadth of knowledge instead of depth of knowledge.

When it comes to social cognition, there are a lot of debates regarding whether the internet provokes the same effects as real interactions would. So far, the studies and evidences show that it does indeed reflect real things like self-concepts and self-esteem. We clearly see this through the neurocognitive responses to online social interactions.

These online social relationships, like any relationships, are connected to feelings of happiness, and mental and physical well-being. Thus being accepted or rejected online feels the same way in the brain, an interpretation, which we'd like to remember, in the offline world is often ambiguous and left to self-interpretation.

However, on social media, unlike the real world, we are presented with clear metrics which give us an indication of whether we fit in or not. They take the form of "followers", "shares", "likes", "friends". The potential can be painful, or addictive because of the immediacy. There is a direct feedback on our self-esteem.

Additionally, the public life on these social media also means that upward social comparisons are omnipresent. People take part in artificial environments manufactured to picture hyper-successful persona. Obviously, this is what the platforms capitalize on. You can go back to the previous section to get an idea.

On social media we aren't anonymous but often create persona, a self-presentation of a real person. One that we mold to be perfect. Everyone has the ability to become an orator, a super-star in front of a gigantic crowd. An online life is like being followed by a million paparazzi.

We know that the medium is quick, indelible, and that a misstep can make us victim of the internet outrage machine. Be it positive, or not, because of private justice or vigilantism, or any other reasons. We are intimately aware of how extreme views proliferate and how ideas are hard to separate — always coming as blocks, hooks, and anchors.

With social media our personal life and work life are intertwined, they come as a package that can't be separated. Our views in one field can propagate and affect other aspects of our lives.

Personal life is now public life, and not only for celebrities.

This is compounded with the feeling of always being scored and tracked. According to the Pew Research Center, 72% of people feel that almost all of what they do online is being tracked by advertisers, technology firms or other companies.

Having private personal details online and our digital reputation can have repercussions in the real world affecting our relationships, job opportunities, bank loans, visa applications, and more.

It is hard to erase something once it is on the internet, and so we apply self-surveillance between ourselves. Indeed, we know our weaknesses are mapped and become increasingly transparent and this leads to self-censorship, conformity, risk-aversion, and social rigidity.

This is a phenomenon called “*social cooling*”. “You feel you are being watched, you change your behavior.” Isn’t this a form of censorship? Privacy is the right to be imperfect and not judged. We’ll come back to this in the last section of the article when discussing some of the solutions.

I was told that I couldn’t be trusted since people can’t check online what I’m doing when I’m not around.

On the good side, the ability to easily get exposure, the appetite for authenticity, and the itch for autonomy have given birth to the *passion economy*.

The passion economy consists of taking the cliché “following your passion” to the extreme. While it didn’t work properly in the past, it is now increasingly easier to achieve, either through an online patronage system or simply because of the new exposure.

The individual is empowered and liberated from previous notions of fixed career path.

The passion economy is centered around purposeful creators that are motivated and driven by their passion, displaying their expertise and experiences with the world.

The audience is as passionate and niche as the creator, influenced and transported through the craft. This is in stark contrast with the apathetic consumers of previous years that made price-focused decision about trinkets of mass productions.

People want to be involved in the making process, they want the whole experience, to engage with the services and ideas they like, to associate with their stories, to build a relationship with the authors. They want to find individuality in their products.

Along with an always public life comes the idolization of hyper-successful individuals. There is a rise in unrealistic expectations of oneself.

Individuation puts the weight on people to find who they are, and it is easy to go back to role models for escapism. These people might in turn use their influence to create a monetizable audience.

The gold rush for scores and fame, the new cult of personality, the new promotional culture going viral.

This is the rise of the “*influencers*” who’ll sell their authenticity for paid product placements and advertisements.

Lastly, these coalesce — individuation, influencers, passion economy, private life becoming public life, and social media — into neoliberalization.

We’ll see more of this later, as it also depends on culture and how people perceive and use the internet in different ways.

This is the ailment of modern society in general, and the internet makes society

more “modern”. A shift in motivations to be goal-oriented and efficient, instead of being based on the more traditional values.

The individuals, with the help of the internet, are now accustomed to marketing themselves as products. This is the modern rule of the game: corporate life merging with private life.

Many products are sold to fill this “*need*”. I’ll digress, as I have discussed this in other articles, and here. We’ll come back to this later.

This concludes our review of the person’s life on the internet in between the corporate, private, and public spheres. We started by seeing how the availability of information is now everywhere and shrinks distances. Then we’ve taken a look at the relationship between networks in societies being mapped online and the effects on cultures. Next we’ve discussed the switch to the information society which creates a need for individuation, networks of people grouping based on their interests. Then we’ve seen how this allows self-generated societies and making our own mind about things. Later we’ve discussed the empowerment of the average person through citizen journalism. After that we’ve glanced at some of the cognitive effects in the realm of attention, memory, and social cognition. Following this we’ve concluded with three subjects: the private life becoming public, the passion economy, and a new extreme form of neoliberalisation that is normalized.

## State Actors: PSYOP, Narrative Warfare, and Weaponized Tech



Geheime Figuren der Rosenkreuzer, Altona, 1785

- Nothing New — Censorship and Propaganda
- Psychology as a Weapon
- Information Society = Information War & Weaponized Tech
- Internal: Population Control, Data and Surveillance
- Computational Propaganda
- External: Cyber Wars
- Social Media as Battleground — State Sponsored Trolling
- Memes as Vectors of Propaganda

Since ancient times, nations have tried to write history from their own point of view. As they say, history is written by the victors. Today, the speed of the internet allows rewriting the narrative in real-time, and state actors will certainly take advantage of this. Namely, there are two ways, or generations, of state information-control practices: an information scarcity approach, aka censorship, and an embracing of information approach, speech itself as a censorial weapon. Both require monitoring of the population to properly adapt the tactic in use.

State surveillance is nothing new either, but the era of information abundance gives the capability of amassing data on a colossal scale.

Historically, nations have used propaganda and surveillance campaigns internally, to control their population, and externally, to sway the opinion of other countries, direct revolts, and other favorable incentives.

Today, these dynamics have moved to the cyberspace. The internet has been part

of all contemporary conflicts as a force acting on the public opinion. Ultimately, the entity that is able to control the media, the discussion environment, the social networking sites, is in control of the narrative.

Before diving into the new era war, let's review how psychology can be used as a weapon.

Psychology has always been used for military gain but got more traction with the concept of total war. This type of warfare includes civilian-associated resources and infrastructure as legitimate targets, mobilizing all resources of society to fight the war, prioritizing it over other needs — an unrestricted war. Thus, having a way to sway civilians in this type of war is a must-have in the fighting arsenal.

Although alone it isn't sufficient and needs to be complemented with simultaneous diplomatic, military, and political tactics. Psychological war takes into consideration the full environmental scope.

A psychological war consists of psychological operations, also known in the contracted form as PSYOPs, which consist of planning psychological activities designed to influence the attitudes and behavior for a political or military objective — to evoke a planned reaction from the people.

This is a vague definition that includes anything we've seen from the previous influence, propaganda, and persuasion section. These tactics, when used as weapons, will be backed up by important state incentives making them more powerful, and arguably more successful, than when they are employed by other entities.

In a total war the target can be individuals, civilians, organizations, groups, or governments. The audience needs to be well delineated and studied so that the message is appropriately formed, as we've discussed beforehand. There are four audiences to a message:

- The ultimate one, the real target.
- The intermediate one, which are likely to receive the message and could be part of the target audience.
- The apparent one, an audience that seemingly appears to be the target but isn't the real intended one.
- The unintended one, which the planner didn't intend to reach but still received the message.

The receptivity, as we've kept saying, depends on many cultural and environment factors. However, in a military setting and with government sponsorship, vulnerabilities can be artificially created through means such as kinetic (bombs and guns), non-lethal biological weapons affecting human psyche and mood, and physical threats. The full environmental scope comes into play.

These operations will employ the schemes we've seen such as anchors, hooks, and imageries. They will be delivered through different methods, and will have a clear aim. The objective is either a positive one — to reinforce the behaviour and feelings of friendliness —, a negative one — to destroy morale, weaken the

adversary, create dissonance and disaffection —, or to gain support from the uncommitted and undecided.

When faced with a new weapon, states have to develop defensive systems. These include doing PSYOPs on their own population, censorship, and counterpropaganda. Although some countries have laws that forbid applying psychological operations on domestic grounds and on their own citizens.

Nonetheless, most countries have integrated in their military structure distinctive branches that are specialized in the type of operations related to the information and psychological sector.

Here is a generic definition of the role of such unit:

The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making while protecting our own.

When deployed these well-trained units can apply these tactics at multiple levels.

- Strategic: applies to anything outside the military area, even in peacetime, to prepare the global information environment.
- Operational: applies to a joint military operation to help achieve consistency between the national objective and the objective of the coalition who they are partnering with.
- Tactical: applies to on the ground operations, especially when facing an opposing force, to support the actions of a tactical commander.

What's important for these units is to be able to measure the effectiveness of their operations (MOE). In military, if it can't be measured then it's no good. The internet offers clear metrics and is the perfect ground for that.

The ethics of these methods is arguable. Some say that it's an arms race and that they are forced to apply them, that the development is unavoidable. Others say they offer a way to reduce the "*significant loss of life*". As with anything, there's a lot of subjectivity when it comes to these.

In an information society, information is the center of the new-generation war and thus these operational units are put to the forefront.

Information superiority is a must to win. Everyone fights for their narrative.

This new generation war is often referred to as the 6th one, where the aim is to destroy economic potential, not take part in physical battlespace, and be the dominant information holder.

Like the information society, this type of war is network-centric, taking into consideration the inter-relations between bubbles and how affecting one could lead to a quick victory. This requires information superiority to be able to plan in advance, conceal, and prepare the multiple aspects that will jointly create a

favorable ground for the goal of the operation — to easily make a nation ply to your intentions.

From information, moral, psychological, ideological, diplomatic, economic, and so on, these are all required. Practically, this means using mass media, religious organizations, cultural institutions, NGOs, scholars, etc.. In today's world this translates into using the right influential methods, and influencers on social media.

The data that is available on the internet, and particularly social media, can be gathered, stored, and linked, to finally become an armor or weapon in the hands of a state entity. It is a tool that can be used both defensively and offensively.

This intelligence gathering often take the form of social media surveillance. The information can be used to identify possible bad actors or individuals vulnerable for a PSYOPs campaign.

On the defensive side, a prominent explicit example of intel gathering is how the USA is now asking VISA applicants to submit five years of social media handles for some selected platforms.

However, the intel gathering probably happens most of the time unbeknownst to the data subjects. This is what has been revealed by internal whistle-blowers, and by more explicit state requirements like ISP keeping internet connection logs for at least 2 months in some countries.

Additionally, we need to remember that social media platforms are “*independent*” businesses. As such, they are bound by the legalities of the geographic areas in which they want to operate. Consequentially, governments can pressure them by taking the legal route and force them to act a certain way to operate on their legislature. Or they can simply buy access to that data from data brokers. For example, it's not uncommon that the platforms will have to obey when receiving an order to censor certain messages. Sometimes notifying users, sometimes not notifying them, according to the transparency rules of the platforms and the legislation in which it is operating. This is the simplest method to get rid of dissidents and keep order in a country. However, for the citizen of information societies, censor isn't looked at too well. The people are craving honesty and individuality, while rejecting authority or association to greater organizations like nations and their wealth, as we've seen in the previous section.

On the offensive side, microtargeting — that is using a conjunction of very specific attributes such as political leaning and interests to target individuals — can be used to amplify a message and have measurable metrics when performing a psychological operation. We'll come back to this topic in a bit.

No need to use forceful actions when speech itself can be used as a weapon. This is what computational propaganda is about, using social media political discussions to sway opinions. Especially that this is the go-to place to discuss these things. This is known as platform weaponization. It can be used internally, to thwart opposition, or externally, to influence the decision-making of other

states.

The act itself could either be state-executed, by the related military branch, state-coordinated, state-incited, or state-leveraged or endorsed.

Computational propaganda relies on the anonymity provided by the platforms which favors black propaganda and gives more credibility, making it seem more genuine. This means that states can deny involvement while inciting or leveraging activities happening on social media for their gain.

Without this knowledge, it is hard to know whether an opponent is attacking or not and how to defend against such attacks.

The attacks can be conducted with bots, automated scripts to scrap and spread data, with trolls, online accounts that deliberately target individuals to trigger and harass them, PR, public relation through news outlets and others, and with memes, which we've covered previously.

Bots, and in particular social-bots, give the ability to create fake online voices, and so to fabricate a public opinion. They are one of the weapon of choice in the cyber warfare of who can shout their narrative the loudest. Online, popularity is measured with "likes", "votes", "friends", "followers", and others which can all be faked.

The advantage that algorithmic campaigns provide is the ability to manipulate what people see, to temporarily boost the visibility of a message, to bypass the social media "*democratic*" process.

Social bots are accounts that impersonate people of a certain demographic, mimicking social interactions on the platforms. These can be used to create a sense of consensus where there is none, or generate doubt on a subject that is supposed to be widely accepted in the target audience.

With the visibility also comes awareness. This can be used by political parties to obtain votes, and to look more popular than others, to look more seductive and attractive.

Another use for such bot is something called astroturfing, fighting for a "turf". This is about creating the impression of grassroots movements in favor or against something, be it an event, person, or idea.

This visibility can be used to choke off debates, smothering adversaries by making it seem like issues are one-sided, controlling the bulk of the conversation. A sort of artificially created social censorship. Trolls can be used for such effect too as we'll see.

Alternatively, algorithmic amplification can be used to muddy political issues, create chaos and instability in the discourse (local or another country), to generate uncertainty, distrust, and divisions.

This is absolutely destructive if combined with on-the-ground actions when discord and confusion reigns in the population, and devastating when combined with economic pressure.

Not all types of content prosper on social media, we've seen that before. We've

learned that outrage and politics resonate well, the things that clash with our cultural insecurities. That is why the bot-led political campaigns tend to come from the most radical parties, it is the most appropriate medium for them. Apart from these, any type of negative content spreads like wild-fire. This is useful to amplify a sentiment of dissatisfaction and disagreement.

In retrospect, social media certainly has some part to play in the process of radicalization, however none of the messages there would resonate if they didn't reflect some issues that were already present in us. As usual, it's an exaggeration of our own ambiguous cultural code.

This is exactly what some state entities use to attempt to influence elections in other countries. Like bots generating discord and chaos regarding a certain topic, microtargeting can be used to personalize messages towards hyper-partisans. In turn, these selected partisans will be pushed into their narrative, radicalized, polarized, and moving the Overton window. Furthermore, this radicalization gives them a bigger exposure and sets the ground for instability in a population. This can be an attractive outcome in coordination with other types of actions.

These hyper-partisans can be converted into trolls, online accounts that deliberately target and harass particular individuals. They can either be paid/sponsored real people or bots, either aware or unaware of the tacit agenda, with or without explicit instructions, and either real partisans or fabricated ones.

This is frequently used along with black PR that are campaigns to deliberately engage in disinformation and harassment against a perceived opponent. It is used to intimidate and silence individuals.

There are countless examples of this tactic being used by states, either deliberately launched by them, or the states harnessing an already ongoing attack. These include, but are not limited to, making death and rape threats, amplifying vitriolic attacks, making accusations of treason or collusion, disseminating libelous disinformation, spreading doctored images and memes, and sowing acrimonious sexism.

The target of these attacks are usually journalists, activists, human rights defenders, and vocal members of an opposite ideology. These types of attacks are used everywhere in the world, some for capitalistic gains, and others for state gains.

Yet another efficient way for states to impose their ideas on the minds is through the news networks, all the headlines. They can employ the typical colored language, the emotive stories, imageries, hooks, and anchors we've seen before to shape the narrative.

Promotional culture is also an important aspect of pushing a narrative through the headlines.

Aside from these, nations can rely on the visibility principle, once again, to promote the stories they want. This could be by voting on social media with bots, or by infiltrating the news network and trading up the chain. News

websites can be constructed from scratch and filled with bogus content, to then rely on the spreading mechanism and citizen journalism to gain credibility and attention. It might finally emerge on the mainstream news media consumed by the desired target audience.

Moreover, trading up the chain can be achieved by using fringe social media platforms which are prone to influence other online ecosystems. This works very well when the message is based on a kernel of truth but with a spin. Even when more reputable outlets are only debunking them, it's giving the content a position in mainstream news.

All these are extremely hard to defend against, a David vs Goliath affair, and so states prefer to defend through a good offense. Counterpropaganda, part of counter-insurgency (COIN), is hard to practice on social media. However, one particular vector of information that can be used as COIN are memes, the new favorite shell for political messages.

Governments are getting more and more interested in memes, especially as a useful method to compact narrative and culture in a transportable container. All modern, arguably post-modern, PSYOPs involve the propagation of memes on social media. Meme wars are an inherent part of political life. We've amply discussed them in a previous section.

They are the embodiment of the competition over narrative, creating coherent constellations of meanings and stories. We know it's easy to overlook them because they are a common way of expression and often use humor, but that makes them the perfect craft for information warfare.

What appears like a prank or trope, soon turns into an influential narrative campaign spread by bots and trolls. Remember that memes aren't limited to their internet format but that they go beyond, that this is only the appropriate envelope they take to move on that medium.

As such, like all that we've seen in this section, they can be used defensively, offensively, and to sway people on the fence, to recruit them or drive them away. They are used both for local and international sentiments.

Many countries employ, or discuss employing, memetics in their military sector. It consists of having separate units in a specialized center for these type of operations, which would be a sub-branch of the usual information and psychological operations but tailored to social media.

These meme warfare centers, or referred to as meme farms when described by opponents, would include interdisciplinary experts such as cultural anthropologists, computer scientists, economists, and linguists.

There are many open discussions about which countries actually employ these units, knowing their associations would reduce their power, but we find implicit indicators in the wild. Most countries and international associations have them in sight, take them seriously, or are actually armed with them already. Nowadays, any side of a conflict will use them, that includes all NATO nations, Russia, Hong Kong, China, Armenia, Azerbaijan, Palestine, Israel, India, Pakistan, etc..

However, it is an unconventional mean and so it is tricky to be put in place, or to let the citizens know it is in place. It is hard to include in a military structure. Memes are abstract concepts and they might sound unconvincing and bring obstacles related to finance — a lack of investments —, culture — the mindset to grasp the new generation warfare —, legalities — to encompass the ethics around using them —, and bureaucracies — who should be in command. Additionally, there needs to be scientific proofs of their efficiency to justify the investment. Efficiency should be tested and measurable, and this isn't straight forward when a change in attitude doesn't necessarily correlate with a change in behavior.

If a nation lacks the framework, mindset, resources, knowledge, and tools, they'll leave the advantage to others that can embrace this new paradigm. Nonetheless, it's apparent that this is a threat but it wasn't until 2017 that the EU and NATO established together a center to counter "hybrid threats". Though its purpose is more analytical than proactive, for them, at least in the public eye, the best form of defence is awareness.

Theoretically, a meme, like a virus, can be categorized in infect, inoculate, and treat. To transmit, prevent or minimize, and contain a message.

A quarantine doesn't really work in the virtual world though and combining this with the neutralization of the infected memoids by killing them in the real world might have the opposite effect. History has shown that it is likely it will instead validate the ideology of the meme.

Detection plays an important role in the defence mechanism, to then be able to launch a counter-message. In practice, it has been attempted for counter-radicalization, a form of counter-insurgency, with mixed effects.

An invisible enemy is and invincible enemy, that is why identifying, cataloguing, and tracing should be done beforehand. Which can be almost impossible when the opponent, be it foreign or local, hides within the civilian population, netizens. Thus, the focus on "hybrid treats" center.

In all cases, displacing and overwriting dangerous pathogenic memes is normally done by replacing them with more benign ones. These reactionary memes have different degrees of applicability, actionability, operationalization, and success. The fruitful reactionary memes have one thing in common: they use humor, irony, and sarcasm to deligitimize the message of an opponent by ridiculing and mocking it. This is similar to WWII propaganda techniques used in cartoons. *"No one is above satire."*

This concludes our review of how state actors are employing the internet narrative as part of their overall information and psychological operations. We've first seen how this is nothing new, how psychology has been used as a weapon for quite a while now, both on the defensive and offensive. Then we've looked at how data is at the center of wars, now that we've moved to an information society. Next, we've seen how this data can be part of the surveillance campaign of states. Later we've examined computational propaganda, how algorithm dictates our world and how consequently they can

be used by nations. Finally, we've dived into social media, bots, trolls, news control, and memes, all communication vectors that rely on gaining visibility and credibility. Speech as a method of censorship, speech as a method of propaganda, speech as a weapon.

## **Biases and Self**

## Cognitive Biases



R. Fludd, *Utriusque Cosmi, Tractatus primi*, Oppenheim, 1620

- Biases Aren't Long Term
- Who
- Physical
- Biases Related to Visibility
- Biases Related to Information Availability
- Biases Related to Social Pressure

Humans are prone to manipulations by their own experiences and biases. Let's review what are some of the cognitive biases and cultural weaknesses that make us fall for all sort of things on the internet.

We've already looked at coercion, deception, and other types of persuasion principles in a previous section. In the following two we'll emphasize on ourselves instead of external factors.

There are many cognitive biases that have been documented over the years, this is nothing new. However, it's interesting to see them under the light of this medium, how they come into play on the internet.

I'll try to list the ones that are the most prominent in my opinion.

In general, biases can affect us when it comes to beliefs, decision-making, reasoning, economic decisions, and behavior. Yet, biases don't have a significant influence on the long run, at least the ones that aren't inherently connected to our cultures. We'll dive into culture in the next section.

Cognitive biases are temporary tricks, temporary stimulations that hack our brain. When someone is aware that another person has used such bias against them, they know they have been cheated. Regardless, studies show that even when trying to influence subliminally, without the audience realising, these types of stimulations only have negligible effects.

In most cases, a bias isn't something that someone creates but something we all naturally have and that is exposed. As such, we can all have them, different

persons having different ones under different circumstances. Kids in particular are more vulnerable to them.

Before diving into cognitive biases, let's stop to mention some physical reactions. In part 2, section 2, we've mentioned social cognition and how communicating on the internet had the same bodily-effects and cognitive responses as other types of social interactions. This implies, as research shows, the same status-to-hormone correlation: stress with cortisol and social confirmation/success with oxytocin, endorphin, and dopamine.

Practically, in the social media environment, which works with interfaces showing quick metrics of social success or failure, that means people's Action-Attention-Reward system will lead them towards addiction. Social media acting like slot-machines — classic conditioning — and keep us hooked.

We all react similarly to these hormones; biased to associate pleasant and positive feelings with what triggers some, and associate negative feelings with others. Hence, we are incentivized to repeat the same behaviors that once got us a dopamine hit — be it finding a niche of expertise we cater to, or posting and finding something shocking.

A market in which everybody has the right to speak comes with the biases of everyone in it.

Some of the biases we can have on social media are in relation to the control over visibility. Biases such as attentional bias, salience bias, framing effect, mere exposure effect, anchoring effect, and others.

Attentional bias is the tendency to pay attention to what is more recent in memory. Similarly, salience bias is about paying attention to what is more remarkable and emotionally striking. The anchor bias is a similar bias, fixating on a single part of a story. In the attention economy we definitely pay attention to what is more extraordinary and recent, and we'll be shown these stories more often.

Mere exposure effect is about being influenced to like something because we are familiar with them, just by being exposed more frequently. Framing is similar, it's about extracting different conclusions from the same story depending on how it's presented. What we are exposed to on the internet is selected by the best buyers, and by our personal interests and stubbornness.

These are compounded into something called continued influence effect, which is a bias related to how hard it is to correct misinformation in our memory after having seen it the first time.

Moreover, our visibility is also affected by biases that make us seek certain things more than others. The automation bias, on the internet, is a tendency to rely too much on the algorithms for recommendations. We know these algorithms are not impartial and can be biased.

While the well-known confirmation bias, illusion of validity, optimism and pessimism biases, are all related to how much we chase, interpret, remember, and focus on information that is consistent and related to what we already believe. We like to stay in our bubble, we are our own filters of visibility with

our biases. We are especially interested in reading and sharing content that connects to our own experiences and senses. These are biases that play a major role with what we'll see in the next section, namely cultural insecurities.

Other biases are in relation to the over-availability of information and how it relates to our memory.

One such bias is the information bias, which is a tendency to look and search for information even though this information is meaningless to us, and cannot affect our actions.

The quest for information is also related to something we've seen in a previous section regarding the extension of our memory. The Google effect is a bias in which we are more likely to forget information if we know that it is readily available online.

Additionally, another popular bias under the name of Dunning-Kruger effect is the tendency of unskilled people to overestimate their own skills. With the whole internet acting as an external memory, it seems like more people are having this bias.

A bias that goes in the opposite direction is the imposter syndrome in which someone with enough experience feels they aren't adequately qualified and fraudulent. With the whole internet pushing forward images of successful and perfect individuals, it seems like some people are more prone to this bias.

The over-availability of information itself can also lead to biases that makes it bypass certain of our defenses. As far as this is concerned, internet memes are an interesting case to examine.

The humor effect is a tendency to more easily remember things that are funny because they both capture our attention, stand out in a flood of information, and make us feel good. Humorous content also takes less time to process cognitively.

The picture superiority effect is the notion that pictures are remembered more easily and frequently than any other format. We've seen that one in the meme section and also said that pictures are processed more rapidly, 60 thousand times faster than text.

There are two ways to process information, through fast thinking or slow thinking, and memes harness speed to skip any form of slow thinking.

These effects, along with content that somewhat goes along with our preconceived views of the world, mean that visual internet memes will bypass criticism, go straight through a peripheral route, and lodge themselves in the brain, to be memorable.

Let's now go briefly over some social biases, which will be helpful for us when tackling the cultural perspective in the next section.

Some of them are related to conformity and others to individuality in a social context. Online, as we now know, social interactions are mostly the same as in the real world, plus instant feedback, big exposure, and a sprinkle of anonymity and fabricated opinions.

When it comes to individuality, the biases of people on the internet are due to the constant exposure they have. For example, the spotlight effect is the tendency to overestimate the amount that others will pay attention to us.

Another bias, in relation, is the reactance: the urge to do the opposite of what others would want us to do, feeling a need to stand out and to assert freedom. It's very common to see this contrarian behavior on social media.

The social comparison bias, yet again related, is about favoring candidates for a position that don't compete with our own. We always compete on the internet, social media profiles are like public CVs and so this bias comes into play.

Other social biases tend to be linked to conformity such as the authority bias, the bandwagon effect, groupthink, and in-group and out-group biases.

Authority bias is the tendency to trust and be more influenced by something or someone based on their origin and perception. We've seen earlier how state actors can abuse this to trade-up-the-chain to reach trusted mainstream media. The bandwagon effect, groupthink, herd behavior, and in-group biases are all linked to preferential treatment to our own group, and keeping harmony, consensus, and conformity in it.

On the other side, there's out-group homogeneity bias where we see members of an outside group as relatively similar. Confusingly, this bias also implies that the members of our own group are dissimilar.

Some people are more inclined to social biases than others. Some will recall images better than others. Distinctive people develop or react to biases in their own ways, be it because of their gender, sex, context, environment, geographical location, professional experiences, life experiences, education, etc..

This concludes our review of cognitive biases and how they get reflected on the internet. We've first seen some of the physical aspects of online addiction. Then we've covered three broad categories of biases: some related to the visibility, others to the information availability, and finally some related to social pressure. The biases related to visibility are about our fixation on what we see more frequently. The biases related to information availability are about what information we seek and how it affects our memory or confidence. Finally, the social biases are about how we conform to a group while still seeking individuality. On the internet these can be used to frame our views, bought or selected by algorithms, decide how information is accessible, and how social interactions get mapped unto social media with an instant feedback.

## Cultural Ambiguities and Insecurities



Alexander Salzmann's 1923 design for institute programmes.

Alexander de Salzmann, cover-design for the programme of the “Institute for the Harmonic Development of Man”, Tiflis, 1919

- Constrained by Platforms or Platforms Constrained
- Beliefs and Values
- Repressed Cultural Weaknesses
- Polarization as a Natural Phenomenon
- Primal Needs
- True Believers

To be a netizen means to be part of the online social sphere. There's no way around it, to have a voice and participate people have to join a platform, which comes with its own limitations.

The rules of the platforms are the rules of the information society but the platforms adapt more to fit us than we adapt to them. Anything happening on them is directly because of real people interacting together. People that have their own hopes, emotions, values, prejudices, and beliefs. Consequently, through our own cultural differences, ambiguities, and insecurities, we are indirectly manipulating ourselves.

We look for confirmations of our own experiences, as we said in the previous section, confirmation bias. We want to share and search for things that relate to our local lives, to make us look smart, empathic, cast us in a positive light,

or that is useful in our day-to-day lives.

On the internet this is proved through many experiments. Emily Falk's Lab, Director of the University of Pennsylvania's Communication Neuroscience Lab, has demonstrated how the expectation of social confirmation and reward influence the likelihood of someone sharing a meme with someone else. We share for social comparison, to look favorable to other group members, for "*virtue signalling*".

Similarly, according to research, on average people visit a maximum of 30 websites before making their mind about something. The bulk of these websites are part of the top results of the search engines of which 70% will always support the view portrayed by how the query was formulated. This is what we refer to as an echo chamber and filter bubble, it echoes back what we think.

We seek information sources that support and reinforce existing attitudes or beliefs, as well as process them. "*All else [being] equal, people seem to prefer not changing their opinions to changing them*" (Lebo & Cassino, 2007, p. 722).

We increasingly, inadvertently through selective exposure by our own judgement, are localized, not only geographically but also through our language, ideologies, time, and cultures. As we said earlier, the internet is made of networked separated individuals, linked by their interests and similarities.

This isn't only about filter bubbles created through algorithms, but it's our natural tendency to pay attention to those who have a lot in common with us. We lack cognitive diversity.

We call this phenomenon homophily, "*birds of feather flock together*". We're really good at it, we have this inner urge to find people similar to us, and this is confirmed by over 100 studies.

This isn't necessarily negative, this allows us to create communities based on niches, on interests, be more democratic, etc.. All things we've seen in part 2 section 2.

We all think that the way we live is the best way to live. We all think that we see the world as it is, that we've come to the best possible conclusion about our direction in life. However, that's just our definition of normality. And this normality isn't even *ours* as most of it happens without us being there. We often can't justify why we do what we do or why we like what we like.

This is as much as about externalities as internalities. We associate ourselves with others like us, as a way of expressing our own individuality by proxy.

We said people spent more time viewing and sharing memes that confirmed their views with others, not only because it confirms them, but also because it's a way of expressing one-self and indirectly promoting who we are. We went over this in the meme section, memes are a representation of our mental models, how we comprehend and make sense of the world.

Ideologies are never force-fed, we are deliberately looking for them. Nobody can be persuaded if they don't want to be persuaded.

That is why when we discussed propaganda we said that the best messages are

those that resonate with the audience, that aren't perceived as propaganda. Not imposed, but emerging from themselves and expressing the concerns, tensions, aspirations, and hopes of the persons.

We live through our media, they define us, we identify with them. That is why the interactions on the internet are a reflection of our different cultures. Everyone has an opinion, however, what is worrying is when they give rise to consequential beliefs. When they manifest in the real world.

On social media, these opinions are now all expressed and openly visible. The pristine walls protecting us have fallen and we are faced with a messy world full of ambiguities.

This is increasingly true when netizens use persona, and even more when they use hide under an anonymous pseudonym. People are then free to express themselves without restraints, breaking accepted cultural codes, expectations, unspoken tensions, and preconceived notions. They aren't burdened by what their peers think of them.

However, we are all biased, as we saw in the previous section, and this confluence of voices brings uncertainty to our own. Doubt sets in when many claim the contrary of something widely accepted. It's also hard for us to accept coincidence as an explanation, which gives rise to some shouting their conspiratorial thinking. Trust is easy to lose and hard to gain.

A trust crisis is setting in.

On social media everyone has an equal voice and different views. We said this was moving us towards a low-context society or informational society. We've also just seen the tendency to regroup in bubbles with people and content that is in agreement with our current views.

Yet, research tells us that social media users have a more diverse news diet than non-users. It shows how much we are bound to encounter opinions and information that might upset us because they go in the opposite direction of our preconceived notions. The bubbles are bursting against each others, and this implicitly creates hostility.

As humans, we tend to connect ideas in a coherent way, to make sense of the world around us based on our culture and routine. We have expectations of what is true, know historical facts set by our institutions, build a narrative from the events we are told, hold public opinions, have pictures of what is normal or not, assumptions about how structures fall into place, and which established powers we think is better.

Yet, again, reality isn't sterile and spotless, these preconceptions are but a thin layer holding a story, and it only covers an infinitely small portion of the existence on this planet. Cultures often have unspoken tensions, anxieties, weaknesses — no story is perfect. This is felt even more heavily when they clash on the internet.

A truth crisis setting in.

These contradictions need to be accepted and that might generate cognitive

dissonance in some people. Cognitive dissonance is a word used to describe the effects someone feels when holding contradictory beliefs, ideas, or values and it's denoted by psychological stress. The human-psyche wants to be consistent, otherwise it creates discomfort. We feel an urge to resolve these contradictions.

Then it's no wonder that some content go viral, it's because they're unleashing a repressed cultural agenda. Online discourse promotes outrage because we feel the need to defend or attack our positions so that our world view doesn't shatter — to keep our own consistency or to find it again.

If we didn't have issues in our societies, these extreme forms of discussions wouldn't materialize. Thus, it is reductive to point the finger at just the social media platforms, that's why we're pointing it at ourselves here.

When facing an unclear situation, a tension, a question, or decision, we instinctively take stances. Naturally we either are with or against. We put ourselves in camps. At least, the most prominent and outspoken people take sides, so on the internet these are the ones whose voice break through the noise.

That person will be exposed to a disproportionately large amount of info similar to their view and a small amount of info against their view. Naturally, they'll want to react the contrarian viewpoints to defend what they think is right.

After that dance, opinions will be polarized and the diversity of point of views and nuances will disappear — the system will have reached its equilibrium.

Absolutist thinking is in human nature when there is an absence of certainty. We want to grasp for reassurance.

The researcher Cass Sunstein has shown that this is even more apparent when putting people that have similar mindsets in the same room. They divide themselves according to more polarized version of the same mindset.

Initially the group shows a lot of internal disagreement over issues but then, again, fall unto an equilibrium. People held more-extreme positions after speaking with like-minded individuals and were more homogeneous, squelching diversity. Either an all or nothing, a black and white vision, highly moralistic, with expectations on us and others.

Similar studies show the same results and adds that people have a less negative perception of opposite views if they get exposed to them more often, instead of mainly the ones confirming their own.

We've seen that people self-sort and seek confirming views online, this widens the rifts between different points. The internet makes it exceedingly easy for people to move into extreme absolute positions and versions of whatever is discussed.

The internet, and particularly social media, also fills the voids that our societies cannot. Gaps in our primal needs: the need for certainty, the need for identity, the need for belonging, the need for accomplishment, competency, and approval, or higher spiritual and moral callings. All things that are missing in contemporary civilizations according to Charles Taylor.

Our lack of certainty about fundamental assumptions and loss of control inclines

us to the middle but opinions on extremes look steady and we slowly move towards them — a need for closure, narrowing our perception.

We generally adopt the first belief that fills the gap, which is given to us by the flashy promotional culture or fringe ones.

These fillings do not have to be understood but believable, to look consistent and absolutely certain. The quality of the ideas themselves play a minor role but the meaning and confidence that they bring matters.

The persons the most sensitive are the ones who are bored, feel powerless, have insecurities in their culture, feel uneasy about the ambiguity of the world, and are frustrated. A feeling of anomie.

They are driven primarily by hope for a coherent future, their gaps filled by the ideology, being consoled and rewarded for taking part in it.

They go under the name of fanatics, highly motivated individuals, defenders of culture, true believers, memeoids, or hyper partisans.

The transformation or indoctrination can happen slowly over time, through repetition and a slippery slope, as we said, reaching a target level of saturation creating a full universe of meanings. Then stuck in a feedback-loop.

Undeniably, microtargeting can be used to find these individuals which needs aren't filled by society, to then turn them into true believers. Monitoring posts can give us insights on whether someone feels stressed, defeated, overwhelmed, anxious, nervous, stupid, useless, and a failure.

It's not surprising that this is going to be used because hyper partisans are the most motivated, they are driven by their ideology and occupy a bigger space in the information market. This is a sort of tyranny of the minority, which drags people that are undecided.

Sarah Golding, the president of the Institute of Practitioners in Advertising, says *"It has essentially weaponized ad technology designed for consumer products and services. There is a danger that every single person can get their own concerns played back to them"*.

Cognitive dissonance and uncertainty open a window of opportunity to hack the mind and bring these individuals in.

The memeoids are known to self-isolate into fringe communities. Ironically, statistically these communities, with their extreme viewpoints, are the most influential on the internet. This is all unsurprising because they offer certainty and answers for the lost netizens.

Additionally, these communities always have gatekeepers and look enticing. They isolate the members and shun anyone that has a different opinion. The stories are reinforced through time. This reminds us that certain communities on the internet are no different from cults, and of the reasons why people join them.

This concludes our review of cultural angst and how they are reflected on the internet. First of all, we've talked about how the internet has its limitations but is more shaped by us than we are shaped by it. We've then dabbled

with the concepts of beliefs and values which always get confirmed through the results given by recommendation/curation engines and other algorithms. Next, we've seen how when cultures clash they make us feel discomfort and bring to the surface cultural anxieties and weaknesses, thus we react. After that, we've talked about how polarization is natural, how we instinctively take sides to become more homogeneous. On the internet this creates rifts between ideas, people want to take sides. Later, we've covered how the internet can fill needs that aren't filled by societies, be it a need for closure, accomplishment, belonging, or approval. Finally, we've looked at hyper partisanship, how people get stuck in these communities, and why they are the most vociferous online.

## The Big Picture



Another effect we've looked at before is how the internet changed the way we retrieve information and value knowledge, acting as a transactive memory — an externalized memory.

The result is that we remember more where to find the information rather than the information itself. We know less about factual information because we've offloaded it to this new medium.

Hence, when we have decisions that rely on facts it makes us dependent on the internet. This can be both beneficial and harmful, as we said, giving us the opportunity to focus on conclusions, emergent hypothesis, overall aspect rather than facts. However, it also makes us focus more on opinions, trust the first results to our query (usually confirming our thoughts), ask fewer questions related to facts but questions related to individuals and society, and put an emphasis on fads and trends.

Our decisions are thus slower, having to consult online resources to make them, and hampered by what someone else has written about the subject we're looking for.

We've previously also seen that social media had the same neurocognitive effects as real life social interactions but with an instant feedback through clear metrics. Time is now objective, not subjective, anything to turn us into machines. This has a direct impact on the concept of the self and self-esteem, making us pay attention to social judgement and social comparison. We've talked about influencers, hyper-successful individuals, and the unrealistic expectations these can create.

These can make us feel inadequate, especially for people that can't manage properly their emotions.

Another aspect that gives us cold feet is the over-reliability of the medium. We're deeply aware that nothing disappears on the internet, that any faux pas will be remembered.

Yet, we've also never been as uncertain about anything. We're constantly the spectators of theatrical clashes of opinions and it makes us doubt our own.

Moreover, we're constantly overthinking, overanalysing things, we are submerged in information and can't take decisions fearing we'll make the wrong ones. An analysis paralysis due to the infobesity.

Joining these ideas related to judgement makes us stay on the bench. These are compounded in phenomena like social cooling, the 1% rule, and lurking.

Social cooling is the self-censure that people exert on themselves because of social pressure. The tension between always feeling watched by surveillance algorithms, knowing our personal data is gathered against our will, understanding that our weaknesses and flaws could be exposed and used against us, and fearing how we'll be scored based on the whims of the internet crowd. We're intimately aware that our digital reputation is now serious business and can impact our real life.

For these reasons, people change their behavior and adapt to whatever makes them look better on the platforms, have better scores or avoid doing anything

that could add a negative side to their reputation. We hesitate before making a move. All over, it makes an environment socially rigid with risk-averse people that conform.

A chilling effect on society and a powerful form of control.

This is in direct relation with the notion of lurkers, a silent majority of passive users that is said to constitute 99% of the internet, according to the 1% rule, and that doesn't participate in the creative aspect.

The vast majority of people only consumes and doesn't contribute any content. This participation inequality has been researched, verified, and shown to be consistent on different online forums and wiki pages such as Wikipedia and others.

There are multiple reasons why most stay on the periphery as read-only users. Social cooling plays a big part in it and the studies make it clear.

When asked why people only observed and did not participate, the common reply is that they were gathering cultural capital: the knowledge that enables an individual to interpret various cultural codes. We take the time to evaluate the implicit and explicit norms of the group, to learn if we can fit, to understand the preferred method of interaction without making mistakes and avoid being rejected, to see the topics of conversations that are allowed, and to learn the conventions of the community. This is commonly done by finding the typical figures representing the community, the models to adopt, templates that exhibit the kind of dialogues we can have.

People also lurk because they fear being redundant or that their contribution would not be worthy. By lurking they can glimpse at what has already been said and done.

We want to copy, belong, but also be unique, that's something we've already seen in the biases section. Maybe it's because our human experience is so similar and yet distinct.

Lastly, people stay afar because they feel that browsing is enough for them. That could be simply because they are looking to find particular content from a place and nothing else.

On the psychological side, lurking is associated with loneliness and apathy, a sense of not belonging. Lurkers are found to be less satisfied and experience more distractions, they are distant.

In the case of social networking, they experience less intimacy and feeling of personal well-being, and an overwhelming loneliness as they watch others participate in the community.

Social media does indeed feel cognitively similar to amplified real life interaction. This is akin to a TV audience but with the sense that what we see is real and not a fabricated reality.

What makes someone de-lurk is situational and depends on both the individual's personality, the environment, and the community. What remains is that only a handful of superusers generate the vast majority of content.

Research shows that these contributors are highly motivated, feel a sense of duty, attachment, and belonging to their online community. Other research show that active participants seemed to be more extroverted and open, felt they were more empowered and in control of their environment, had confidence in their ability to influence, had higher self-efficacy, and a greater need for gratification.

That is in sync with what we've seen regarding frustrated individuals that had their cultural malaise and gaps filled by the internet. Participants need a place to express themselves and that is relevant to them.

Statistics show that the people contributing the most are out of the ordinary, they exhibit extraordinary behavior. That means that when we consume any content on the internet, we're mostly consuming content created by people who, for some reason, spend most of their time and energy creating this content. These people clearly differ from the general population in important ways. The kind of people that move the Overton window, which we talked about. This is worth keeping in mind when on the internet.

Knapp, had been submitting an average of 385 edits per day since signing up in 2005 as of 2012. Assuming he doesn't sleep or eat or anything else (currently my favored prediction), that's still one edit every four minutes. He hasn't slowed down either; he hit his one millionth edit after seven years of editing and is nearing his two millionth now at 13 years. This man has been editing a Wikipedia article every four minutes for 13 years. He is insane, and he has had a huge impact on what you and I read every day when we need more information about literally anything. And there are more like him; there is one user with 2.7 million edits and many others with more than one million.

These days the 1% rule has been more or less debunked as the barrier to engagement has decreased. However, it hasn't decrease enough, the number of lurkers is still relatively high and social cooling adds to the equation.

This paradoxical balance between lurkers, conformity, social cooling, and out-of-the-norm influencers and contributors in different communities, makes us feel a sense of normalcy and lack of innovation.

Normalcy is the consequence of adherence and conformity. We lurk because we want to adhere to the norm, not stand out, to fit in. We're also interested in participating because of the homophily phenomenon we've discussed before, "*birds of feather flock together*".

This all keeps the status quo and homogeneity in the community.

This creates a situation in which we're offered templated, cookie-cutter identities which we can choose from, and indirectly coerced to fit into them by the persuasive technology. It's easier to market to persons that fit into well-separated categories, to "*buyer personas*". One could even call these memplexes and memeoids, honed through eunemics.

This is all decided by fads, opinions, and interests, a sort of “choose your character/future” mode of identity building. With these templates there’s an emphasis on attitude rather than facts, truth, or moral. Sometime called “*Hypernormalization*”.

*“How can you have a personality if you have no knowledge to base it upon, and if you merely have opinions that have been given to you through slogans or clichés.”*

It is hard to get out of a template, these mass one-sided personalities, because of all that we’ve seen before especially the social judgement, social cooling, the action-attention-reward addictive mechanism, and others. We need privacy as a right to not fit in, a right not to be perfectly molded, well-behaved, docile, and conformed humans.

We are guided by biased algorithms that are mathwashed, believing they are impartial.

This has detrimental effects on kids that are in the process of finding themselves, in the process of building their personality. They feel enormous social pressure to be perfect. Self-inflicted injuries, such as cuttings that are serious enough to require treatment in an emergency room, in the USA, have increased dramatically in 10- to 14-year-old girls, up 19% per year since 2009.

Less physically harmful, is the effect on young boys that are looking for achievements and get addicted to “*competency porn*”, any type of media that fulfills the need for recognition, achievement, and control over the environment — Be it video games or animated movies. The epic tales and escapist fantasies of today’s world.

It is astonishing because different persons are part of different internet realms, with different templates, and are given skewed pictures of reality — it’s as if everyone lived in alternate universes that sometimes, but rarely, cross.

Indeed, even though the UN considers the right to internet access a human right, the effect of the globalisation of the internet are unclear.

Already we’ve seen filter bubbles, homophily, and confirmation bias that keep people within the same realms. Additionally, we have to add to this the privileges associated with the internet. Not everyone can access the internet, not everyone can use it powerfully, not everyone can participate in community content creation, and not everyone has the language skills to participate in these various communities.

The content is still subject to being part of a hierarchy, still based on the same social and international hierarchies that exist today. Minority views in the real world are still minority views online, the same people facing discriminations offline also tend to face them on the internet.

And yet, it also fosters the democratization of speech if used properly, but the content we are given somehow reinforces the status quo.

It’s a global and local presence, we could say a glocalization. Everyone that has internet uses it in their own way, and the way they use it affects their perception. Some use the internet for research, some for hobbies, some to socialize, some to

learn, some as a tool for work, etc.. Internet usage is shaped by the myriads of ways that we access it for our needs and values.

Yet, this exact habit of usage is shaped by the local culture and thus also creates a divide as the internet is inherently based on connecting networks together.

For example, even though we can use the internet for different things, the language we speak will only give us a narrow view of the whole spectrum. If we search using a language that is more “popular”, let’s say English, we’re prone to be given the templated identities related to the most vociferous online English speakers (USA).

Language then is part of the dynamic of who defines and who is defined.

There are other imbalances that exist based on geolocal preferences. For instance, speakers of a certain language will prefer domestic issues.

Moreover, advertisers, the main source of revenue online, will prioritize specific consumers that fit a template from a certain culture and geographical area, and not others. This will incentivize content creation for that specific audience, as this is where more money is made. This in turn will widen the cultural gap, now a digital advertising gap, thus a media content quantity and quality gap.

There are many factors that make the internet both global and local at the same time. Again, it depends on our usage of it but when we default to the average person, there’s no room around being presented only narrow views.

The question remains whether internet truly makes people conform, what’s the state of creativity and counterculture, and how much propaganda comes into play.

The literature shows that a small subset of the population, around 2 to 3%, have international ties and act as bridge figures between cultures. These persons show a higher creativity than their peers because of their exposure to different views.

From this we can imagine that it’s the same thing on the internet.

When using a service you become part of its ecosystem, there are many platforms and the big ones, the FAANG, have a tech hegemony. Internet in itself didn’t kill counterculture, it is just not present on these platforms as they encompass a sort of new overarching powerful entity, sometimes more organized than governments.

This means that counterculture today isn’t any more about a war of ideologies but about going against the trends of the internet. The counterculture of the past, which rotated around personal expressions and identity are now used by platforms to drive engagement and profit, it’s part of their lucrative business. Social media in particular have been catering to the “demands” of a generation by filling the gap that the culture couldn’t — self-fulfillment as a product, as we’ve seen earlier.

This means that these types of old countercultures are still part of the system, but by embodying them we’re not in charge. We pull ourselves together by gathering pieces of templated subcultures. Then, this collection becomes our

niche personal branding, our personal expressions and ideologies.

As we went over in part 2 section 2, we are now seeking individuation, we are networked individuals connected by interests. This is in stark contrast with counterculture which requires a group to thrive, an “*us against the world*” mindset. The internet does allow regrouping but only on a shallow level, particularly for collective dissent and dissatisfaction, turning the groups to absurdities and cult-like behavior.

Directly opposing the system will only make the system stronger.

True counter-culture can either be found by embracing the algorithms, understanding their inner-working and warping them to our needs, or by signing-off and rejecting the whole system for an alternative one. Both of these are difficult in the era of like-and-share.

So we are bound to use the internet, and the internet to project our anthropological nature, its current state and flaws, be it conformity, homogeneity, or others.

We’ll be given a reflection according to the function it has for us, our lifestyle, current society, culture, and time. For a big part of the world that means the internet is becoming inherently neoliberal, used for neoliberal ends, and encourages neoliberal behaviors.

This isn’t surprising considering the origin of the internet, who are the biggest internet companies, and who are the most vocal online. The internet embodies the “*American mindset*”, a mindset of personal brands and marketing, the self-made man.

A considerable amount of people are driven by this, with different subset cultural bubbles living outside the hegemony of these giants because of different environmental constraints.

The internet is the perfect tool for the workings and reinforcement of neoliberalism values. It is a perfect display of how this way of viewing the world, which was heavily questioned during the Cold War, has taken over.

It focuses on a certain flavor of democracy, individualism, and a laissez-faire absolutism of the marketplace. The belief and undeserved faith in the efficiency of markets. It centers around deregulation, free trade, privatization, and puts the individual at the center of everything. Any other attitude, and especially government intervention, is frowned upon.

We can clearly see how this has unfolded on the internet, with Facebook’s many scandals clarifying the limits of corporate self-regulation.

There’s an over-emphasis on economic efficiency and growth at all costs. Political theorist Wendy Brown has gone even further and asserted that the overriding objective of neoliberalism is “*the economization of all features of life*”.

The self becomes a product, a personified capital that needs to accumulate symbols of status, a storyline, and advertise itself. With regards to the internet, and because the money is where advertisers and the audience put their interests,

a personal-brand will only be profitable if it fits the mold of the popular culture. We have to partner with the brands and products that make us shine. We own things that reflect our personal meaning. We calculate the benefits, efficiency, and productivity of each action. We had a look at this in the new economies section, this is in relation to this. The commodification of personal data and attention for profit.

This unfettered exploitation puts gains before anything and it doesn't only apply to individuals but especially to corporations. That is why marketing is prioritized on the internet, an optimization of products and surveillance. We de-emphasize public goods to turn our eyes towards the market idolization, a corporatocracy.

Everything has a monetary incentive rather than a social objective. Anything needs a metric, an indicator, to be tracked and quantifiable. This focus on economic efficiency can compromise other, perhaps more important, factors, or promote exploitation and social injustice. We see this on the personal level on social media through likes, shares, and subscribers.

It's arguable if neoliberalism, the advent and rise of this way of life, are bi-products of the internet or if it's the opposite. It's arguable if individuation is the product of neoliberalisation or vice-versa, and if they are accelerated by the internet.

It's probably a mix of everything, societal changes with the private enterprises reflecting the will of individuation of private individuals, which are also projected on *their* internet — the internet driven by the big players.

We'll see later how these societal change and acceleration bring social unrest.

The individuals are at the heart, all the responsibility and weight are on them, that's why they focus so much on identity politics and individual gains, while dismissing broader identities and class consciousness.

A mix of looking for authenticity, as it seems to be the gap in cultures that have embraced neoliberalism, and an overwhelming majority of narcissistic individuals.

A mix of losing political freedom because of apathy, and looking for self-fulfillment as withdrawal from moral concerns. Are lurkers neoliberal? Are counter-culture and creativity now anti-neoliberalism?

Globalisation doesn't necessary mean homogenisation, but it's undeniable that the neoliberal mindset has spread further than any other and can't be dismissed. Its acceptance, normalization, the incentives, indirect influences on the internet and its dynamics are apparent.

Isn't this the best propaganda, one we don't even notice unless we're someone in the middle, someone cross-cultural?

Nonetheless, what happens online is only a function of the offline status quo, the offline paralysis. The internet does not exist in a vacuum. It is made with the purpose of letting people connect with their own networks, assuming that users are individuals, and inherently individualising them.

The online world recreates and accelerates — there is nothing inherent within the technology that makes it neoliberal, it's only a tool. Each can have their own different internet experience depending on how they use it, as we kept saying.

We're both formatted and free individuals — freedom as a menu.

This concludes our review of how the internet has consequences in the acceleration of cultural evolution, formatting individuals, paralyzing them, imposing an overwhelming homogenisation while letting fringe people contribute, and fostering and spreading the neoliberal mindset.

At first, we've examined the cognitive effects: attention, memory, and social cognition. Our attention is divided, our memory externalized, and our social fear amplified. Then we've seen how the internet makes us constantly anxious of making indelible mistakes, embodied in the concept of social cooling and self-censorship.

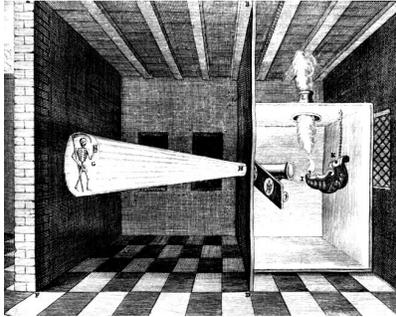
Next, we've observed the link with the notion of lurkers, read-only users, the 1% rule, and the out-of-the-ordinary users that actually contribute the content. These contributors do so because the internet has filled something they were missing, a cultural gap.

After this we've questioned conformity and homogeneity, how the internet offers template we select from, and puts pressure on individuals to fit perfectly. Yet, we've also observed that these templates, these experiences, and the internet function as a whole, differ and are divided per culture, environment, language, and others — the glocalization of the internet.

Later, we've added to this the fact that the internet is driven by monetary incentives and that it will create a dynamic in which more content is targeted at people that fit certain templates and others will be enticed to fill the templates of other cultures, an indirect cultural assimilation.

Following this we've discussed what it would mean to stand out of these templates, of all these memplexes, to be more creative or counter-cultural and we've concluded it means either embracing the tech or going against it. Finally, we've linked the topic with neoliberalisation and how it exemplifies the phenomenon we're seeing, both by emphasizing the market, efficiency, and the individual.

## Truth and Trust Crises



A. Kircher, *Ars magna lucis*, Amsterdam, 1671

- Individualism, Neoliberalism, And Relativism
- Lack of Trust — Doubt as the New Normal
- The Collapse of journalism
- Mobs and Self-Justice

Nobody likes to be put in a box, nobody likes to be paralyzed. In a world where the individual is put first, we want to feel in control. Yet, we are lost in a whirlpool of chaotic and clashing ideologies, memplexes and absolutist templates. Who are we, how should we define ourselves? This makes us distrust any form of authority and renounce classical forms of media. As individuals, we're looking for authenticity, whatever form it can take even if disingenuous, so that we can find our new roots, our new base. Then, there's nobody better suited to affirm justice than internet mobs.

It feels like the internet is the new far-west, a lawless land of incessant doubt, lacking meaning and trust, where gurus, inspirational influencers, and vigilantes reign and data, personal data, and metrics of reputation are the currency held by the banks of social media.

Or it may also feel like eunomics in action — the deliberate improvement of the meme pool — and people wanting to take part in the cultural meme wars and genocides.

A lot of this can be attributed to the wide spread of neoliberalism values and mindset, which as we've seen in the previous section are the most prevalent online. Particularly, we're faced with individualism, relativism, and inequalities all justified by the protection of personal rights.

If you see a world full of individuals then you'll want a morality that protects those individuals and their individual rights.

You'll emphasize concerns about harm and fairness.

But if you live in a society in which people are more likely to see relationships, context, groups, and institutions. Then you won't be so focus on satisfying individuals, you'll have a more sociocentric morality.

Which means that you place the needs of groups and institutions first, often ahead of the needs of individuals.

If you do that then a morality based on harm and fairness won't be sufficient. You'll have additional concerns. And you'll need additional virtues to bind people together.

#### *The Righteous Mind*

The individual becomes reason in and of itself, and not only a figurant in their own life. We are expected, in the neoliberal theory, to develop our own opinions, outlook, stances through a considerable amount of solitary reflection. However, most important issues, such as the definition of our identity, happen over dialogue. We can't define ourselves or recognize ourselves, in a void. We've discovered how this can be beneficial in part 2 section 2, as networked individuals connected by interests. Interests become part of our identity and how we generate meaning.

On the internet, however, this leads to struggles as we're incessantly exposed to a wide range of ideas, some of which may be breaking our local taboos. The Overton window keeps moving, for the better or the worst.

Isolated societies, communities, and ways of living may be forcedly assailed by ideas outside their comfort zone. We've touched this topic in the cultural malaise section.

I went a bit over this in my article entitled cross culture frustration.

The new mentality appears different and frightening — different acting, different social dynamics, different manner of building the "self", different definition of who we are within the society. In addition, we hate being wrong, and we like confirmation. We create a cocoon and hide ourselves in it repeating the hokum over and over again. And we are afraid of the unknown — afraid that the stable self we've built to be part of a society is not a self that could partake and feel comfortable in the activities of another society.

In this mindset, the individual always comes before the large collective forces and needs to be protected against them. Personal life choices can't be criticised as this would be tantamount to an assault on personal dignity. Inherently, this carries the acceptance of a soft moral relativism, any opinion should be respected and nobody should impede on others.

This translates on the social plane into political acts for individual rights, recognition, and equality. Anything else is understood as inflicting damage and being a form of oppression. We are more interested in dignity, universals, innate attributes, and equality.

Additionally, this requires the breaking of hierarchies and a loss of a grand sense of meaning. The perception is now centered on the self to find these, rejecting, and even erasing from awareness, issues and concerns that transcend the self. We aren't recognized through honors, distinctions, or any rare achievements, but by our self-generated worth. We've replaced these forms of recognition, the need for belonging and authenticity for example, by other things.

Personal and intimate relationships are now the definition and emphasis of life. We now expect to find the greater meaning, which was previously found in institutions and traditional structures, in these relationships. The domestic becomes the loci of "the good life".

This is the core of what social media are about. They are filling a cultural gap as we said before.

Self-fulfillment and worth is also found through the instrumental reasoning of neoliberalism — actions driven by profit, optimization, market, and metrics. Meaning lies in efficiency, success is found in numbers, tangible assets, products, and money. In a way, it has replaced grand narratives and sense with short-term narcissistic, selfish, pleasures and pains, with little regard for others or society as a whole.

Similarly, the intimate relationships are also seen as tools for self-development and so are also serving an end.

It permeates every aspect of life. Even simple things such as food have become an individual matter, for personal consumption, rather than a convivial mean of regrouping and conversations.

Old social orders are shattered and replaced with resources for projects, economic growth, and prestige in technological progress.

No empathy. No loyalty. No forgiveness. Thanks to the market, the old-fashioned virtues have been rendered obsolete.

Common goods and social objectives are de-emphasized. The protection of the individual is only an extension of the protection of their private economic rights. The new morals are the morals of protecting the individual and their economic rights, the sanctity of the individual and the pursuit of self-interest as the highest moral ideal.

However, this system generates a lot of inequalities, there's a wide distribution of wealth and income. It is hard to keep competition open and fair — a competitive attitude that also fosters more individualism. Corporations are free to self-regulate.

Comparativeness and cooperation are both part of human nature, but the one that is valued and promoted by the culture will thrive.

On the internet we're presented with the myth of individual geniuses working in their garages without any investment, self-made success stories. Yet, this is only a myth.

And because worth is found in such success, it is then displayed in clear light

for everyone to admire. Social media make this even more apparent. These inequalities will undeniably boil into social unrest. Individual persons will demand their individual rights and feel entitled to do so.

Overall, there's a sentiment of being stranded on an island, lost, afraid, and missing something vital. Many societies embracing or exposed directly or indirectly through the internet (or other political pressures) to neoliberalism have a hard time coping with this. The competitive and instrumental mindset encourages a fear of the other. The moral relativism destroys grand narratives, old societies heroes, and replaces them with ambiguity and an identity crisis. The cultural malaise, the feeling of anomie, we've discussed earlier. We're left with defining ourselves through interests, intimate relationships, metrics, economic activities, and a moral that only has one thing to say: *"everyone is on their own, let them be"*.

We are like islands in the sea, separate on the surface but connected  
in the deep — *William James*

More than anything, this damages and erodes our trust in any form of authority, this makes us doubt what we know and what others are telling us. We've seen how this is abused on social media in a previous section.

When reality doesn't reflect our projections, it will backfire. Turning things upside down, changing love into hate, or any other ways of rebalancing our perceptions.

We project on people, ideologies, cultures, and politics, wanting to put our trust in something, to see them as extensions of us, to feel that our conception of reality is stable and secure.

When it doesn't match the people revolt.

On social networks we are torn between different narratives that threaten each others. There's no accountability or regulation for this user-generated content and it is often published under aliases that can't be traced to any source.

Truth and trust are bent to their extreme. The digital revolution undermines mainly the control that governments used to have on them, replacing it with a technological alternative of wild-west, open, democratic, and sometimes manipulated discussions.

Infobesity and infoxication don't help either, we're inundated and can't keep track of what is important, nor absorb it, nor understand it, nor know who said it. It makes it hard to effectively grasp issues and make decisions, as we've discussed in the paralysis section.

We've also previously seen how state entities are trying to get back the control by using speech itself as a censorial weapon.

The biggest consequence of this is that there has never been as much political discussion happening. It's everywhere on the internet and it is what thrives. However, the memetic material, the content, is always provocative, conflicting, shocking, and sensational because, as we keep repeating, this is exactly what thrives in the internet environment, namely: what touches our cultural sensitiv-

ities.

Consequentially, in relation to what we said before, this content will be about identity politics and identity in general, personal definitions. Discussions will rotate around recognitions of who some people are, the gaps they have in their cultures, how they patch them, the oppressions and damages they feel are being done to their previous or new-found identities.

Some discussions and content are more powerful and dangerous than others, activated ideologies that have real world consequences. This can lead to warranted or unwarranted protests, extreme ideologies, discriminations, assaults, suicides, acts of violence, and others.

In a previous section we've dabbled into how this can be used and initiated as part of PSYOPs.

This becomes alarming when doubt engenders the creation of an alternative reality that contests well-accepted scientific truth and facts, turning virtue into a vice. The lack of trust in authority being replaced by a trust in narratives that claim pseudo-authenticity and certainty. Sometimes coming from ill-informed people or from nations or entities that have an agenda — misinformation and disinformation.

This is what we've talked about when discussing memeoids, propaganda, and cults: a memetic equilibrium, a coherent world of cohesive meaning. The grand sense of meaning that was broken with neoliberalism but that couldn't be recovered through anything else. The modern hermetism, or return of mysticism.

Doesn't memetics itself reflect the concept of neoliberalism, all selfish memes fighting for their individual survival?

The word "truth" is often semantically associated with some religious or moral doctrines. This confusion also occurred in psychological literature.

In practice, this is embodied through conspiracy theories, built over time on the accumulation of confirmation biases and wishful thinking, and also through polarized and absolutist memetic wars that carry new narratives.

The side effect of these is the collapse of the classical form of journalism. Traditional media in its original shape is dead and along with it any form of "*official narrative*".

There exists some media that are government owned, publicly funded, but the netizens do not trust them.

The online economy has ravage journalism. For example, in the USA, about a fifth of newspapers have closed and the survivors are shadows of what they were. The ones that are left rely on shock value to drive revenue from ads, the new business model, or have switched to subscriptions. Many geographical regions are now news deserts leaving people to rely on social media instead. This results in the dramatic decline of professional reporting, yet a majority of people have not, and will not, notice any significant change.

The dominating ad networks, Google and Facebook, have their own alternative news channels and also decide on the internet dynamics: promoting or demoting a newspaper based on its popularity and how much revenue it attracts.

Citizen journalism is now king and the traditional media are following their footsteps, redefining themselves as intermediates. Social media platforms have replaced the gatekeepers, as we've seen earlier, and the "democratic" curatorial systems decide which news are important and how they get framed.

While in the past the news were responsible for what they said, regulated, limited by their journalistic values, now it's fully unregulated.

There are upsides and downsides to this new development. As we said, these are amateurs, people without journalism training, and so the quality of the reports and coverage can vary, is subjective, heavily opinionated, unregulated, and can be abused by malicious actors — such as spin doctors.

However, it can also promote human rights and democratic values to have the people join together and collaborate in this endeavor.

We've tackled before how the engines reinforce what people already believe, amplifying their narrative through their self-generated (and often fabricated) news.

It's even more distressing when heads of nations publicly attack the press, calling them "enemy of the people", inflaming opinions, polarization, and partisanship. Politicians have learned how to play the game on the internet.

Along with the self-generated meaning and self-generated news and facts, we see the rise of self-justice, private justice.

Ironically, this is in stark contrast with what neoliberalism is about, it is the large collective that fights individuals, the return of the battle of the collectivist narratives.

The polarization with its absolute us vs them mentality. A return of a sort of absolute moral rigidity with categorical imperatives.

Laws should be there to protect minorities, not lead to mob violence, and vigilantism, the kind of fast justice, with total impunity, and auto-defence that is justified by militias around the world — the wild-west and absence of authority that favors the creation of these dynamics.

This lack of trust in institutions and truth makes us want to create our own. We substituted the old gatekeepers, so we can also redefine the social contract.

Corporations and multinationals have been doing this for some time now, pushing their own justice, influencing legislations, spying, and thwarting competitors using any means. This has definitely been facilitated by social media.

On the individual side, it's understandable, we're presented a world, through the lenses of the news and social media, of constant chaos, clashes, and protests everywhere. It seems to be the only logical conclusion, when doubting all authorities, that we should fight for our own rights and that no one else will do

it.

The offline consequences of this are apparent so let's talk about the online ones.

The collectivists narrative, one that sees each person as a member of group and not an individual, a kind of "*social tribalism*", is the way people bring back order from the chaos of getting exposed to different ideas — a pre-neoliberal view within a neoliberal mindset.

It is associated with a make-belief of simple dichotomies, groups at war, enemies, activism and counter-activism. Societies then become a struggle for power, a zero-sum war of ideologies. These ideologies are, within neoliberalism, related to identities.

Some of these are hijacked or pushed by political actors for gain. This is by various kind of parties that adhere to different political ideologies on the political spectrum.

This forcing of homogeneity, is the same force that drives indoctrination, cults, and memeoids. On themselves, these distorted worldviews and conflicts are wars of memeplexes, each side carrying their package of culture.

The combatants fight to annihilate the other memeplexe, to achieve eunemics — essentially trying to deliberately control the meme pool.

The war of memeoids is fought by quarantining other memes, restricting their speech/thoughts through censorship, and also done by executing attacks that ridicule memes to detach them from the enemy's memeplex.

*"Tyranny is the deliberate removal of nuance."* – Albert Maysles

Only one reality must survive!

When it comes to these attacks, they are filled with derogatory terms, loaded words that carry with them cultural ideas, politicized insults: essentially memes in the form of words. As we said, ridicule and satire are the best tools to fight narratives and drive discussions.

Creating a new language is also creating new ideas. Satiric words are thus both attacking memes toward the enemy memeplex, and new memes to be incorporated in the memeplex of the generator. A memetic warfare. Benjamin Lee Whorf said: "*Language shapes the way we think, and determines what we can think about.*"

A lot of the popular words are taken from the USA politics, so we'll extract some examples from there, any reader should be familiar with the terms considering their invasiveness in the online sphere.

One of these words is *SJW*, "*Social Justice Warrior*", a pejorative term used to describe someone who promotes "socially progressive views" for personal validation rather than conviction. This word carries a political meaning in the USA politics, is a satire thus a meme.

The term itself is used by the opposite ideologists to refer to the internet combatants of the other groups. These *SJWs* rely on victimhood talk, a twist on the oppressor narrative along with emotions, to silence/censor their opponents. Absurdly, the groups using the words are themselves portraying

the world in a similar way, the back to the collectivist narrative.

The personal validation is described as “*virtue signalling*”, a way to show your virtues and allegiance to a group. Virtue signalling is the common phenomenon we’ve seen happening when people share memes on social media: informing and showing others that they belong, that they know what is right, following what they think is prestigious, along with a sense of superiority.

It is most often used to point out “fake outrage”, “political correctness”, “microaggression”, “microinvalidations”, and “self-righteousness” (also meme terms), but it can also be applied more generally to anything used to get social karma/points.

Indeed, this is related to the neoliberalism narcissism coming from finding meaning through metrics. Obviously, and contrary to popular beliefs, this noisemaking is done by anybody on the political spectrum and not only by a single political camp. Only the association and its cultural reference that packages it in the name makes it a novel meme.

*“In a democracy, recognition matters. Everyone wants to be seen as they are. If they are not, then it’s impossible for them to enjoy the experience of being full citizens.”* — Melissa Harris-Perry

The term is also associated with slacktivism, hashtag activism, and pathological altruism. These are ways of supporting causes on social media while not involved in the on-the-ground activities and the messiness. These are terms used, and mostly prevalent, by Western netizens to describe how they are distanced from reality and act from the clean pristine cocoons of their sofa.

They are pejorative because they imply that these actions have little effects, might even be ineffective, are low-cost efforts, and can’t substitute more substantive actions. However, as we’ve seen over the past sections, we know that online political talks do indeed have an effect on mindsets and allow for more discussions around a topic — temporarily getting attention, selecting what is important.

One technique that is extensively used today by all groups, political parties, or association as a defense mechanism is a sort of deliberate social cooling of others, a self-surveillance that goes by the name of call-out culture and cancel culture.

The names are normally used by a specific political side in USA politics as a derogatory term describing another side, but the techniques themselves are applied by everyone anywhere in the world. It’s about using the online-outrage machine we talked about earlier to attempt to defame and vilify characters that go against the memplex of the group.

This public lynching type of censorship should be a reminder of the propaganda we’ve seen earlier. Speech as a censorial weapon.

A perfect way to achieve eunemics through the suffocation of memplexes.

This concludes our review of the truth and trust crises accelerated by the internet. In a first part we’ve seen how neoliberalism and individualism have shaken our notions of stability and broken our vision of authorities and hierarchies.

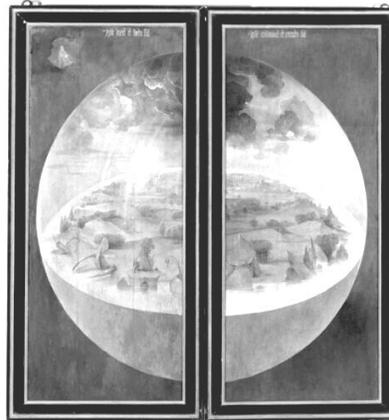
The individual is favored before the collective, and they now find meaning through metrics, economic activities, and moral as a protection of new personal identities. Next, we've looked at how this unbalance can backfire if projections don't match reality, especially when presented with so many worldviews on social networks.

Then we went over how this generates an enormous amount of political discussions, especially related to identity, and how this generates alternative universes of meanings that live on social media, some of it conspiratorial or based on novel narratives. A kind of self-generated meaning.

After that we've observed the collapse of traditional journalism and all that it implies, especially that now people can generate their own news, their own facts.

Finally, we've concluded with a glanced at a self-generated justice, a private justice created through the return of a collectivist narrative, fights between groups. These groups being memeoids, that fight eunemics wars on the internet trying to annihilate other memplexes using some techniques we've encountered in previous sections such as speech as a censorial weapon.

## Mass Hypnosis or Mass Psychosis



Hieronymus bosch, outer wings of the Garden of Delights, c. 1510

- Relations With Well-Known Dystopia
- Attention, Awakening
- Mind Control and Mass Hypnosis
- Alienation and Mass Psychosis

The internet brings with it technological advancements that remind us of dystopia that sci-fi writers have talked about. So let's go beyond what we've tackled so far and project ourselves in hypothetical futures to posit bigger consequences.

The two archetypical stories of dystopian futures are *Brave New World* by Aldous Huxley and *1984* by George Orwell.

In *Brave New World*, Huxley presents a hedonistic future that is governed by techno-science and eugenics. The people conform and adhere to the societies rules for the following reasons:

- The future of people is predetermined based on their genetics, their place is chosen and what makes them happy too.
- The people are conditioned in their sleep, while unaware, to find certain perspectives more enticing and to always be happy and satisfied of their position.
- It is a future in which pleasure and happiness are everywhere, and it makes everyone prone to accept the status-quo. Who will rebel against pleasure?

We can see some parallel with neoliberalism, consumerism, and the passivity or paralysis we've seen earlier. However, we've also seen how people can't deal with such world of templated lives, even when pushed by the internet.

Mass production, homogeneity, predictability, and consumption of disposable consumer goods.

In *1984*, Orwell presents a world of constant surveillance by Big Brother. This surveillance is extended through self-surveillance between individuals with a thought police. The world described is believed to be in perpetual war (forever war), historical facts and news are rewritten or negated to fit the accepted narrative, and language is used in a powerful way to accompany it. The fictitious world employs many of the propaganda techniques and the eunemics we've encountered.

We can see some parallel with the previous sections related to the surveillance economy, the return of the collectivist narrative, and the internet wars of memplexes that use censorship, call-out, canceling, and social cooling to keep everyone in check.

In one of these worlds facts are eliminated and in the other facts don't matter. Today we see both of them, censorship and speech itself as a censorial weapon. Two techniques used to make people docile and well-behaved, two techniques that are omnipresent on any communication channel but even more on the internet. We're in the center of an information warfare.

Beyond dystopian worlds, the attention economy on the internet carries with it questions related to the very nature of consciousness.

When we talk of attention we also indirectly refer to themes such as awareness and awakening. These are then tied to spiritual practices. For instance, how we pay attention is an inherent part of Buddhist practices.

Hence, attention can be said to be the outermost expression of our consciousness. Losing control of it would be the equivalent of losing oneself or being detached from reality and be brought into a fabricated universe.

Some have come to call this the hyperpresent.

In an attention economy, we would then live in memplexes of ideas, packaged, wrapped, and opened effortlessly to let us access these collapsible concepts, these portable philosophical ideas, stories, emotions, narratives, and meanings. We are what we focus on, we live what we are aware of. Our reality is limited by our perception of it.

We all think that the way we live is the best way to live. We all think that we see the world as it is, that we've come to the best possible conclusion about our direction in life. However, that's just our definition of normality. And this normality isn't even ours as most of it happens without us being there. We often can't justify why we do what we do or why we like what we like.

When we spend so much time on the internet, and will possibly spend much more in the future, we're indirectly unaware that it is defining us.

Looking around us, for some it might appear more explicit than others as they get caught in apparent internet cults or are memoids combatant of their memplex, but aren't we all?

Isn't most of the content that is fed back to us a reflection of who we already are? And as the internet takes a bigger part of our lives, will everyone get stuck in loops of paralysis like we've seen before?

One question we can ask is whether it's possible to engineer these wants, to use mind control or hypnosis to make people more inclined to give their attention or perform specific actions.

A far-fetched, or not so far-fetched, concept from sci-fi is a psychotronic weapon or electronic harassment. This abstract weapon is a representation of the totality of all possible methods and means, be them suggestive, pharmacological, paranormal, technogenic, or others that influence the psyche of a person for the purpose of modifying their consciousness, behavior, or health.

While this idea is often associated with lunatic conspiracy theories, it's interesting to tinker about the possibility that the internet could indirectly be used in the future, or now, for such ends.

One way to be able to achieve this would be to get a direct interface to the brain. The neurotechnology for brain scanning, which used to be limited to laboratories, is slowly getting more accessible, transportable, and less invasive. There are instances using electrical activity circuits, rhythmic sound or flashing light, ultrasonic or magnetic simulation, all to modify brain waves and patterns of electrical activities in the brain. These can work both as reading devices or output devices.

Today, these are still used mainly in labs to treat neurological and mental illness, and improve mood and cognition. The USA FDA has approved in 2008 transcranial magnetic stimulation to treat depression, pain, and migraine.

However, we can imagine that when this becomes more mainstream, when brain-related data starts to be common on the internet, that ad-tech companies will jump on the opportunity to access whatever comes out of these new body sensors.

There is nothing more private than thoughts. This can give the ability to know and predict what someone's mental dispositions are, with whatever this implies: from knowing their cognition style, to identifying cognitive strengths and weaknesses, to perceiving personality traits, and to determine their aptitudes or likeliness for certain information.

When in the wrong hands this could be called a *neuroweapon*.

Having this type of information in the wild would be the most advanced form of social cooling, full-on paralysis, a forced "psychocivilized" society, not far from Huxley's brainwashing dreams.

This is why researchers and human rights activists are starting to think about

adding new rights: cognitive liberty, mental privacy, mental integrity, and psychological continuity.

Another method to alter minds that has been tried in the past is by using chemicals and pharmaceuticals drugs. The research has shown, at least as far as the public knows, that they aren't very effective and their applicability comes with a lot of technical difficulties.

Some mind-altering and stimulating chemicals are already readily available on the market of most countries. Others such as hallucinogenic mushrooms, marijuana, heroin, LSD, and truth serums aren't as available everywhere but the intelligence community showed that they weren't effective when it comes to applying a particular military objective or operational deployment. This is because their effects isn't reliable nor the information that people give when under them — people could become drowsy and spurt out fictitious stories.

Yet, we can imagine that these can be used without a particular goal but with a more generic approach. This is why some of these are now being introduced and tested as psychiatric drugs to treat anxiety, depression, or mania. They force people to enter new states of minds and emotions. Many of them work by returning overactive or underactive neural networks and signal to more “*normal*” levels — a reset button on the brain.

These drugs can also engender the opposite effect and actually increase confusion, anxiety, and depression. Some military have been using them for torture to force the person to cooperate or surrender.

An additional topic in relation to mind control is hypnosis.

Hypnosis is a state of awareness where someone detaches their of attention from their environment and get absorbed by their inner experience, their feelings, imagery, and cognition. These inner experiences and imageries are induced by a clinician that will guide the process.

The imagined feels real in that state, bridging the gap between the left and right hemispheres, the hypnotic reality. Similar to a trance state or meditative state, an obliteration of the ego.

Three things happen in the brain of the hypnotized person:

- The activity in their salience network decreases, a place in the brain related to worry, so they get absorbed in the moment.
- The brain-body connection increases.
- There's a reduction, even a disconnect, between the actions and the awareness of them.

As we said, this can be seen abstractly as a link — by using imagery — between the left-intentional brain (logical, rational, abstract, critical), and right-involuntary-state brain (emotions, feelings, instinctive, intuitive).

In practice hypnosis is studied and used along other forms of therapy such as CBT (Cognitive Behavioral Therapy) to fix misbehavior. It is used to increase the effectiveness of suggestion, give access to the mind-body link and

unconscious processing. Alone it is not very useful, but it facilitates other kinds of therapies.

Hypnosis can be self-taught but it is most often administered by a clinician. It starts with a relaxing phase where the patient focuses their attention, giving it away, an induction step. This could be done in multiple ways, be it a visual focus or auditory one. The next step is a suggestion phase which consists of the clinician guiding the patient by helping them create a visualization of events and scenarios, be it verbally or using imagery, to help them address or counteract unhelpful behaviors and emotions.

In a sense, this is very like guided meditation where someone sits in a relaxing position, calmed by a mantra or sound, and is guided by a master that will help them address their inner woes.

*“In hypnosis, you’re so absorbed that you’re not worrying about anything else.”*

However, studies show that only a minority of the population is hypnotisable, about 10-20% are highly receptive to it. It has been shown that hypnotisability is a genetic trait and follows a Gaussian or bell-shaped distribution. So most research related to hypnosis focuses on this part of the population.

Now, related to our main topic, this doesn’t seem like mass hypnosis would be possible, nor very actionable either. Yet, we can imagine a world in which daily activities, wandering online, becomes a trance state and where imageries are transmitted using compacted packages such as memes.

Still, that is far from the truth as most studies show that it is almost impossible to make someone do something against their will. Moreover, only an extremely small part of the population would be both willing to do *“evil”* biddings and also be susceptible to hypnosis. But wouldn’t these fringe people be easily findable on the internet and band together anyway?

Homo homini lupus.  
Men is a wolf to men.

When the psychology of a whole population changes it can create a deleterious unstoppable snow-ball effect.

Indeed, it is becoming ever more obvious that it is not famine, not earthquakes, not microbes, not cancer but man himself who is man’s greatest danger to man, for the simple reason that there is no adequate protection against psychic epidemics, which are infinitely more devastating than the worst of natural catastrophes. — Carl Jung

When a society loses the grip on reality, becomes driven by uncontrollable fear, when mental illness becomes the norm rather than the exception, social alienation takes over, a psychic epidemic.

All one’s neighbours are in the grip of some uncontrolled and uncontrollable fear. . . In lunatic asylums it is a well-known fact that

patients are far more dangerous when suffering from fear than when moved by rage or hatred. — Psychology and Religion

Mass psychosis happens when a large portion of society descends into delusion, similar to what happened during the European witch hunt.

It is a paranoia taken to the extreme caused by a rise in anomie, societal stress, and a flood of negative emotions.

*“A mysterious, contagious insanity”.*

We can already see how this can be amplified on the internet where these types of emotions, ambiguity, confusion, fear, and doubts thrive. We’ve discussed amply the cultural insecurities and cognitive dissonance in the previous sections.

We can also wonder if these can deliberately be induced in another population through PSYOPs.

Don’t we also see the rise of this phenomenon through the memoids and their memplexes, taken over by ideas so powerful that they possess them, consume them, even destroy them? Mobs and self-justice carnage and destruction.

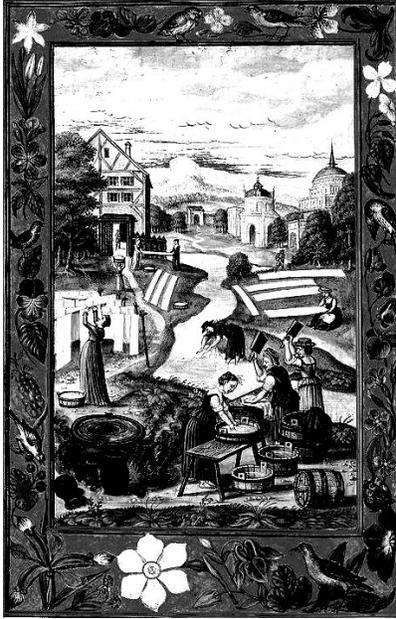
Moral absolutism, and categorical imperatives are cognitive distortions because most of reality and the living of everyday life takes place in the gray area, between the extremes.

Those who control the flow of information in a society, the ideas we accept as true or false exert a great power over the course of civilization.

This concludes our review of future societal meltdown, be them hypothetical sci-fi scenarios or realistic ones. We’ve started by taking a look at the relation with well-known dystopian stories such as *Brave New World* and *1984*. We discussed the parallel with today’s internet, censorship and speech itself as a censorial weapon. Then we’ve talked about the deep inter-relation between attention, awareness, and consciousness. We’ve said that a control of attention is a control of reality but that online we’re often only given back what we already want. Next, we’ve wondered about different ways to engineer the “wants” of a person, from mind-control weapons, to getting access to data taken directly from the brain, to drugs and chemicals, to hypnosis. Finally, we’ve discussed mass-psychosis, the state of a society where mental illness becomes the norm and reality is distorted to fit an invented narrative.

**Adapting**

## Free Market, Let it Solve Itself



S. Trismosin, Splendor solis, London, 16th century

- The Market Will Decide
- Promoting Fair Competition
- Privacy as a Feature
- Changing the Economic Dynamics

In this last part, we'll go over the adaptations we are undergoing to remove the frictions we have with the internet — anything to make it better suited for us. We'll take multiple perspectives, primarily the ones of users, societies, and others that are encountering the issues we've seen related to this new communication channel.

Let's start by taking the point of view of the market and economy as ways, in themselves, to provide solutions to problems we've had.

Keep in mind that these heavily depend on the locality, culture, and practices of the tech companies at the epicenter of the internet drastic changes that are taking over the world. Most of these giants embody a neoliberal mindset and originate from the USA.

A market solution is a solution based on trusting the free market before all else. It hinges on not having to intervene with regulations and laws but to believe

the behavior of consumers, their choices and decisions, will eventually lead to an ethical and moral balance.

This laissez-faire attitude is anchored in what we've seen in the cultural ambiguity and truth and trust crises sections. They rely on the assumption that individuals understand the dynamics, are well-educated on the subject matter, and will always make the best (economic) decisions overall.

This line of thinking is contested, but let's consider the adjustments and innovations that can be driven by users.

Market solutions are hardly international as they can only work by relying on fair competition and transparency between actors. Non-intuitively, at least in the eye of some, this can only be achieved through some regulations that keep the market in checks, and such regulations are geographically bound.

When it comes to the online world, because a lot of the money is made from ads and tracking, it means regulating the whole digital advertising tech supply chain, and data brokers along with their partnerships.

If this isn't done properly, there could be conflicts of interests, some companies self-preferencing advertisements for the services they themselves provide. This is relevant because many of the ad-tech providers also offer other services, which they can promote through their ads to compete with other players.

This problem is exacerbated when only a few entities, which as we know is the case today, have the upper hand (hear by that almost monopoly) in the ad tech sector and data broker space. These companies can then thwart competitors by buying them or competing directly with their services.

The companies will then accrue larger datasets and it'll be harder to compete with them. This is what we've seen in the new economies section. They can control the pricing and quality of services on this digital supply chain.

To promote fair competition, to make it a free market, many things can be done.

One of them is to break the large datasets into subsets to allow new smaller entities to compete instead of having systems of interlocking monopolies.

Another thing that can be done is to manage conflicts of interests, which is what some lawmakers are doing these days. This includes institutions such as the European commission, the Competition and Markets Authority in the UK, the Australian government, and the USA Congress that are now checking for risks of collusions, antitrust, and what can be done for fair competition. We'll see more of the law and regulatory concerns next.

Additionally, one thing that can foster good competition is to have open standards describing what can be done with ad tech, the format of the data traveling on the pipeline. This includes implementing a common transaction and user ID for consumer and making them portable and interoperable across ad providers.

It would then be easier to port the data between rivals and might even allow consumers to regain control over their data, selecting with whom they'd like to

share it. We'll see more of that when discussing digital identity.

Apple uses something called IDFA, Google uses an analytics and advertising tracking ID, Facebook uses a Pixel ID and others.

Standardization also goes along openness such as the right to repair, to allow products to be repairable to last longer, and decentralization.

However, openness can also be abused for profit. We've seen countless times that standards that are initially open can be hijacked. The big players will in turn drive the standard towards more complexity and growth, consequentially kicking out any small player that can't follow.

This is arguably what happened in the "browser war", and is still happening today with web standards. The ones contributing the most will control and subdue them, while defending their actions on the basis of openness, improvement, and progress.

History also shows that the same companies that emerged thanks to openness tend to reject these principles when they undermine their strategic position. After gaining a substantial amount of users, after being rooted deep enough, they'll use the network effect to justify changing their tactic and stance.

A too big to fail scenario.

Obviously, companies can also spend money to defend their interests, for example by lobbying the USA Congress, as we've seen in the new economies section.

There are many ways to make money online, on the internet market.

To make profit, as we've seen in the new economies section, the most popular models are the ones that go along with what users expect, namely zero-price models where data is exchanged instead of money. This goes under different names such as "free model", "data-as-payment model", "online advertisement-based business model", "ad-supported model", "freemium model", etc..

There are other models that are possible, as we'll see, such as a flat-rate model with unlimited or limited usage, a bundle-like model, and a per-usage or subscription based model where users are enrolled and charged recurrently.

The names for the free models actually have separate particular meanings that reflect how each view and make money from the data, personal data, or attention, which become the currencies of exchange. These models also provide insights into manners of approaching privacy.

The consumers are then free to select the model that they find the most suited to their needs, interests, and ethical concerns.

The ad-supported model, one in which companies make money from selling ads or from gathering data for ad-tech providers, poses the most privacy concerns. It is either targeted advertising, such as microtargeting, or context-based advertising.

A freemium model is one in which the product is offered free of charge and money, a premium, can be paid to access additional features or services.

The free of charge part can be combined as a hybrid with advertisement.

A data-as-payment model, aka PDE or Personal Data Economy, is a model in

which individuals deliberately sell their personal data as an asset to pay for services and products. This model turns the surveillance economy upside down. Similarly, a privacy-discount model is a model in which the users relinquish their privacy to obtain a discount on a product or service.

These two models are user-centric, letting the consumers take back a semblance of control over their data: with whom they share or disclose it, the price for it, and on which terms.

Each model has a different perception of what privacy is, either as a commodity/product/feature, as a luxury/premium, as a right, or as a utility.

In the market view it is primarily a feature or premium that can be transacted.

What we described as data-as-a-payment or privacy-discount are instances of perceiving privacy as a commodity. In these scenarios neither citizens nor governments care about privacy regulations but freely exchange and trade it. In this case, people are powerless about what information is being transferred, while tech companies can make huge profits by selling the data.

Privacy can also be seen as a luxury or something you get for a premium, aka PFP or pay-for-privacy, aka premium aka privacy-as-a-premium. In this scenario, consumers are encouraged to pay extra to gain back their privacy, or to acquire new products that will fill their desire for more privacy and security. This is a case where companies profit from privacy by charging users for it. Transparency, awareness, and privacy have become competitive features delivered at a premium.

We'll see that awareness and transparency are two things that can be enforced through laws in the next section.

On the other side, privacy can also be seen as a utility or universal right. Either something the governments regulate, control, and monitor, just like water, a tool — this is what we'll see later with digital identity. Either as a universal right that needs to be protected by law, which is something we'll see next too.

The debate over privacy can be confusing for consumers, they may feel torn between all these options. Some of them wanting to disengage with the virtual world to maintain their anonymity instead of putting themselves at risks. Without privacy, we are subject to social cooling, feeling tracked, caught in the polarization, as we've seen before.

This confusion is indeed what sparked the whole branch of privacy as a luxury, companies are capitalizing on it, for them it's a new business opportunity.

Privacy is not only a feature in itself but also a stand, a brand, a show of force for publicity and marketing differentiation.

Many companies sole existence rely on this need: selling something at a higher price mark because of this or having products, devices, services, and tools, that will offer control back to users.

The market size of this type of business, according to Arthur D. Little, is estimated to be, as of 2020, around \$5 to \$6 billion.

VPN providers are one category of these flourishing businesses. They sell a

service to avoid the continuous online tracking and data collection. A VPN being a proxy to internet requests, essentially hiding where they are originating from. Some commentators have suggested that all consumers should use a VPN. In general, their model is based on offering a subscription, a pay-for-privacy product with recurrent payment. Though, ironically, some VPN companies also provide their services for free through the hybrid “ad-supported” freemium model.

Another company profiting from privacy is the device and OS manufacturer called Apple that sells products at a premium. It has recently (2021) stirred uproar from American companies that make money from the ad tech infrastructure and pipeline when it announced a recent update to their phone, tablet, and TV OS. Apple is a popular product in the USA among high earners, thus good ad targets.

The recent update would notify users when applications want to access location, track them across apps and websites, or others. The user would have the choice to allow or disallow such action.

The move is arguable, as Apple makes a lot of money from the ~30% cut (the Apple tax) it takes from in-app purchases, disallowing any other type of external purchases linked to apps. Such a change would force app developers relying on the ad model to switch to another model such as subscription or in-app purchases, which they’d take a percentage of.

As can be seen, the free market and laissez-faire approach brings with it a lot of conflicts. When big players can enforce business models on their platforms, after using the network-effect to acquire users, it enrages other players.

The dynamics at play are interesting.

When privacy is offered at a premium it raises concern about the inequality of acquiring it, a socioeconomic digital divide. “Advertising is a tax on the poor”, as Scott Galloway said. It creates incentives for the companies offering privacy and security-centered products to keep the status-quo, to make more money from it.

There’s also the lack of consumer knowledge and understanding on these issues and their implications. They could either be unaware that these are issues, or be misled by marketing schemes portraying products as privacy-aware while not providing any proof to back it up.

Privacy can be advertised on the front while in the back tracking is done. The tracking, the telemetric gathering, is not limited to advertisement purposes but could also be used for partnerships with other entities that would allow companies to gain an edge. For example, a partnership with state actors, internet providers, or mobile operators.

Let’s remember that companies are not moral agents, nor arbiters of truth, and that their decisions are both restricted by, on one side, the legislative geography they are operating on, and on the other side, the profit made from the appearance and satisfaction they offer customers. Ethics is only a cosmetic feature.

This can be hard to grasp for the neoliberal mind that tries to find their meaning through the purchase of products, as an extension of themselves. Especially when these products only provide that in return of profit.

One solution for consumers is to go toward models that remove data from the equation, thus changing the economic incentives for online businesses. These alternative models rely on putting real value on what we consume and use online, going back to transacting money for intangible assets.

While the free models were disruptive when they came out, it turns out, unsurprisingly, that consumers don't like being harassed by constant ads. Tech aware users will often install ad blockers on their machines, rely on one of the above paid solutions to not be tracked, use browsers that block third-party cookies, and other mechanisms. We'll dive more into the tech solutions later. Statistics show that in the USA 47% of users use ad blockers.

This kills companies that rely mainly on the ad model. Either because they aren't able to attract enough users to generate revenue, or because it damages the brand image.

Additionally, companies don't want to be at the mercy of the ad tech monopoly, which puts them at risks when they decide on the budget and price they allocate for specific ads and on which platforms they'll run them. They could demonitize them at any time or disallow them on the ad platform for arbitrary reasons. Furthermore, even companies paying for ads are starting to see the limits of this model because of the lack of good insights, bots, and fake information that return to them.

For these reasons, we're seeing the rise on the internet of the subscription economy, micro-transaction economy, passion economy, and the economy of patronage.

We already discussed the passion and patronage economy in part 2 section 2 so let's focus on the others. All these are about putting the consumers in power, letting them make decisions through their wallet. In this case we'll have a consumer-controlled world, thus a working free-market solution.

There are different types of subscription models, either based on usage volume, or based on time via a billing cycle. It stands in contrast with a pay-per-product model where users would pay only once, in subscription the payment is recurrent.

Consequentially, this works well for products that either perish quickly, need to be replaced, e-commerce loyalty programs, or intangible goods such as the ones provided by SaaS (Software as a Service) companies.

These include Netflix, Amazon Prime, Hulu, YouTube, Spotify, SiriusXM, Pandora, VPN services, among others.

The subscription model has been estimated in 2017 to have 28k companies worldwide and had more than a 100% yearly growth. The largest retailers in the category generated more than \$2.6 billion in sales in 2016, up from \$57 million in 2011.

The model has the advantage that it is flexible and provides customer satisfaction. Buyers aren't burdened by large fees and can stop the subscription at any time. The companies providing the services are then forced to innovate, improve, and provide quality to be able to attract and keep customers. There are many instances that show that switching from an ad-based model to a subscription model has helped increase revenue.

Here the customer is at the center and their expectations are king. For this model to work the company has to build a long-term relationship with them, often focusing on the relationship more than the product or the transaction.

Nonetheless, it isn't an easy task. A minimum number of subscribers is needed for the business to subsist, and it's not easy to attract them when netizens are used to getting things for free.

This has especially been hard for newspapers, as we've said in the past. Statistics show that in the USA in 2017, only 11% of consumers were paying for online news. The rest of the world isn't as generous either, the statistics have been replicated in other places with an average of 10% paying for news. Yet, recently we are now seeing an unexpected resurgence, a new growth. It has been reported that in 2017 the American newspapers The New York Times gained 130k subscribers and the WSJ gained 300%, the British newspaper the Guardian has also announced that it had seen profits for the first time after 20 years with more than 300k people making contributions.

The most successful stories of subscription based businesses are those that relied heavily on partnerships — between brands, consumers, affiliates, and others. Despite all this, companies relying on the subscription model can still rely on product placement and advertisements, which puts us back at square one.

Another method to increase the number of customers, to persuade them of contributing, is to lower the barrier of entry. This could mean making it more affordable, or even to change the value of the product based on the purchasing power of the individuals or their locality.

The new disruptive approach is to make the payment infinitesimally small, a micro-payment, a micro-transaction, which can be fractions of cents, there's almost no line of demarcation.

This can create a dynamic in which ads and trackers are unnecessary because users would pay directly with these monetary tokens the online content creators. The tokens essentially being the monetary form of the attention of users.

The word micro-transaction refers to purchasing virtual goods through micro-payments, however it also has a historical meaning attached to the gaming world.

Initially micro-payments acted as a sort of virtual currency that existed only within games.

Later on, some game developers used a model in which they provide virtual desirable assets, such as loot boxes, in exchange for micro-payments. Micro-transactions have thus gained a connotation with gambling and addiction, which

brings some countries' legal matters and regulations in the mix especially when it involves kids.

The main issue with micro-transactions is that they can only be possible if there is a monetary technology that allows real-time transfer, no fees, and privacy. Cryptocurrencies on a blockchain seem to be the go-to solutions for this. They are far away from the traditional pipeline that is also linked to data brokers, as we've previously seen.

Unfortunately, some of the cryptocurrencies have issues regarding scalability and volatility, which makes them ill-suited for such endeavor. Cryptocurrencies are now more attached to investment and gambling than an internet free of ads. Recently, payment gateways and banks have taken a particular interest in trying to gain power in this space. Namely, VISA and PayPal are now allowing certain cryptocurrencies to be used and converted on their processing platform. This would then bring information related to cryptocurrency to data brokers, removing the privacy aspect.

Still, the applications for micro-payments open avenues and unlock an entire economy between subscriptions and ads.

We're slowly starting to see this appear in specialized browsers that allow to distribute attention tokens to websites and content creator, and newspaper that want to allow micro-transactions along with their other revenue streams.

This concludes our review of how the free market can be used as a method to adapt to the internet. First we've seen what this idea implies: well-informed customers making the right choices to balance the status and set things right. Then we've explored how this cannot be true if there aren't regulations set in place for fair competition to happen between companies. Next, we've discussed some of the possible regulations and things that could be put in place to achieve this such as collusion checks and open standards. After that we've set ourselves on looking at different business practices, ways of making money online. Some of them are related to the ad business, others subscriptions. We've tackled how these models offer a glimpse into what privacy is considered: product, luxury, tool, universal right. When privacy is a product it's traded freely. When privacy is offered at a premium, which we called primium, it's done because of a need and not because of moral or ethical standards. We've listed some businesses that base their marketing or product around privacy. Finally, we've seen what removing data from the equation implies: having customers pay again to be able to choose, either through subscriptions or micro-payments.

## Legality, Transparency, Accountability, the Nations Intervene



Michael Maier, *Atalanta fugiens*, Oppenheim, 1618

- Laws and Governments as Moral Arbiters
- Free Market Competition Is Not Enough, Privacy as a Human Right
- Balance Between Sociality and Privacy
- Consent, Ownership
- Consent, Persuasive Tech
- Consent, Right of Non-Reception
- Accountability, Securing Data
- Accountability, Content + Gatekeeping
- Transparency, Processing, Usage, Analytics, and Partnerships
- Transparency, Disclosing Sponsors
- Transparency, Bots
- Example Laws
- Drawback of GDPR
- Standardization of Data
- Privacy as a Utility, Government Monopoly on Identity
- Social Media as a Utility
- Digital Identity, Identity as a Public Infrastructure
- Examples of Implementations

The market and corporate self-regulation have their limits. They cannot in themselves be sources of morals and ethics. This is the realm of laws, the legislations that governments make are the real arbiters of duties and rights. The governments, as state entities, can impose the rules that should be followed to be able to act on their territories. However, laws are bound by geographical areas and as such cannot be international. They can only be inter-governmental

if treaties and partnerships are in place. Companies can decide to comply to different regulations in different areas to be able to operate on these markets.

The best defensive tactic for nations is always legislations, instead of leaving it as a free-for-all medley. This is what we'll dive into: when governments intervene on the internet.

The neoliberal mindset abhors this return to authorities because of the general lack of truth we've seen earlier. Yet, who do we trust more and want to grant more authority to: private for-profit entities on not-so-free markets or our governments and their legal systems?

In this section we'll focus on rights and not regulations related to the private sector. Things related to transparency, accountability, consent, ownership, utility, and identity.

We've already seen market regulations for fair competition, conflicts of interests, collusions, antitrust, and others that are currently discussed or getting in place around the world.

Despite these new market regulations, many of the internet giants and their partners still stand tall and confident that their business model isn't going to fall. Either because of nifty bypassing techniques, or because of lobbying. That's why such regulations don't coincide with what most of the netizens actually want.

For example, many recognize and want privacy to be a basic human right, part of human dignity. The "right to be let alone".

Similarly, we've previously seen how researchers and human right activists are now thinking, when it comes to brain data privacy, of new rights such as: cognitive liberty, mental privacy, mental integrity, and psychological continuity. On the surface, these will only be fancy words of wisdom and considerations if they aren't written in laws, legally binding. Otherwise, companies could lie. Governments have to ensure the spirit of the laws are applied and not mere market regulations. It would be catastrophic if no such basic rights are in place and sensitive personal information such as brain data become common place on the internet.

The question today are related to who's in charge of the privacy and what kind of balance we can have. Can our information be both a currency for some and protected as a right for others?

The actual implementation is a hard problem when it comes to privacy guidelines as there is a balance between sociality and privacy: sociality has always required the voluntary abandonment of privacy. In order to be social we must give up some of our private time and space to share it with others.

This takes new forms online where sociality is taken at the expense of privacy and social autonomy. Today, it rests mostly upon digital records and archives in the hands of private companies that track our social behavior. As we'll see, it could be more attractive to have these records switch hands from the corporate world to the public sector.

The legal world is a tricky one, the laws need to be written so that they cannot be abused, covering as many aspects of an issue as possible to not leave room for ambiguity.

The first clarification that needs to be made is about defining what is meant by personal data and who is the actual owner of such data. We already gave our definition in the data and personal data section in part 1.

Personal data is any information that can be used to directly or indirectly identify a person, an attribute currently attached to them, a behavior, a preference or interest, personal history, anything. These include things such as name, phone number, address, email, schoolbook, credit scores, geolocation, travel logs, interests, information about past purchases, health records, insurance records, online behavior, etc..

We call the person to which the personal data belongs a data subject.

Having this definition in a text law is the starting point.

Then, comes the issue of ownership of the data. As you might remember, we called the person which data was extracted from the data subjects. Hence, we need to specify what are the rights of ownership they have over their data, and in which cases they need to give consent to allow others to access it.

The consent itself needs to be delineated properly. We need to know what can be done with the data, for what purpose, for how long the retention can be, and most importantly, if consent is transferable. One company getting approval to access data could share this data with other entities, the transitive consent and transitive propagation of data.

Ownership also rhymes with control. Laws might want to spell out if a data subject should or should not be able to perform corrections, updates, or erasures of the data they have generated.

Yet, consent makes no sense if people can be coerced into giving it, if it isn't informed consent. This is the case online with the use of persuasive technology, both to extract data and be subject to advertisements. They go hand in hand. Thus, the legal domain has to take this into consideration and posit whether such technology is allowed or not.

Additionally, it could make the parallel with gambling, alcohol, cigarettes, or other questionable products, basically limiting advertisements on mainstream channels.

Furthermore, when it comes to consent, the law has to deliberate if persuasive algorithms and designs should be allowed on children or not — age is often a factor when it comes to consent. Persuasive design and dark patterns could be made illegal altogether.

When it comes to advertisements, it has to be decided if consent needs to be given even before receiving them, or whether the person can at a later time refuse to receive them, retracting it.

The right of non-reception, is the right of someone not wanting to be the

recipient of ads. If such right is in place, companies could be pursued in court and fined if they advertise to people who have opted-out of them, or to those who haven't opted-in depending on how the law is phrased.

Such right is generally associated with online cookies, the right to not be traced online.

Offline, it is associated with not receiving ads in mailboxes, or at city-scale, to not have or limit billboards. This is also a method to avoid material waste.

Still, these can easily be bypassed with an ingenuous use of product placement and sponsoring instead of direct ads. Or even turning customers into brand evangelists, which is the norm with neoliberalism as we've seen earlier.

Once the personal data is stored, it could and is expected to be subject to access restriction and accountability. The companies and entities we have trusted with our data should be responsible for their safety so that nobody else retrieves them.

Thus, governments could create bodies and processes to verify the security, integrity, and confidentiality of the data storage in companies and entities that choose to host it. With the increase in quantity and types of consumer data, it is imperative to have such measures in place. We've heard too many data leaks stories in the news lately, either from hacking or rogue employees.

Arguably, even standards like the PCI-DSS, if applied to personal data, might not be enough without real-time checks.

Along with the responsibility of storing the data, laws could dive into the accountability related to the content of the data itself. Should platforms be accountable for the content it hosts, or should it be the data subjects themselves, or both?

This would in turn create new gatekeepers: a monitoring and reviewing of the content published and hosted. This could also include the algorithms that are used to promote content.

These algorithms have acted as amplifiers of extremism, enlarging dangerous fringe communities, and pushing biases (racial or others). Currently, the entities that are using them have been hiding behind the fact that these are algorithms, and thus "*mathwashed*" removing their responsibility because "*they have no conscience of their own*". The myth of the impartial machine.

Many of the social network platforms, in the USA, have been avoiding monitoring the content posted on them by referring to the USA first amendment of free speech and the 1996 USA Communications Decency Act, shielding them from liability for content posted by their users.

However, this only applies to the USA and the different branches of the same platforms are able to monitor content in other countries.

To thwart this, governments need to either consider social media as news platforms, or find methods to strengthen the institutions that create and distribute reliable information: mainstream media, academia, nonpartisan government agencies, etc..

Once social media are part of the mainstream news system, the gatekeepers are back in place, they'll have to uphold journalism standards for the content posted on them.

Governments can also enforce social networks to pay news that get published and distributed there, indirectly re-strengthening the local media publishers.

Apart from news, the platforms can be held liable for the undesirable content that is shared there.

This is most important when this content is shared in a public space that children can access. Laws can ensure children won't be subject to neither surveillance, tracking, and be protected from predatory and dangerous content. Contrary to popular belief, in the USA the COPPA (Children's Online Privacy Protection Act) only takes the advertisement and tracking of children, but not whether the platforms are responsible for the content to which they are subject to. The Child Online Protection Act of 1998 (COPA, yes similar name) is the one that has the intent of preventing minors from accessing obscene material on commercial websites in the USA.

Most countries already protect their children against being subject to harmful material on public commercial channels.

India's new intermediary liability and digital media regulations takes a step further and forces content to be traceable to its source, to be able to verify social media users, and rapidly take down non-consensual sexually explicit content and morphed/impersonated content within 24h of being notified.

With the same mindset, some countries have laws specifically to take down online hate speech and incitations of violence or terrorism.

If we can't blame the hosts of the content, we might want to hold the people that generated it accountable. This, in turn, should make black propaganda ineffective. However, because most online-interactions are anonymous, it is very hard to do.

A solution to this would be to attach a real identity to whoever uses, posts, and creates online content, this is what the concept of digital identity is about.

Online platforms that allow bots could also be forced to tag them as such, making it clear to everyone that these aren't real humans.

We'll discuss this later, but as you can expect, while it does bring back gatekeepers, it also could create more social cooling.

Agreeing that the personal data should only be used for specific purposes is fine, but there needs to be some guarantee behind the agreement. For trust to set in, transparency is mandatory.

One type of transparency is about understanding why and how the recommendation engines, the curation systems of the internet, work. From advertisements, to news feeds and other algorithms. Having a clear picture of their inner-workings would help us make better decisions and responsibilities instead of overly relying and trusting them.

With the recommendation engines come the analytics, the categorizing, ranking, rating, and scoring of data: how data is processed internally. Transparency is

about knowing where and how our data will be used, in what process. It could be hard for companies to accept transparency at this level because that would mean opening their valuable extracted data storage to the world.

The transitive propagation of data needs also to be transparent if it happens. That includes disclosing who are the third parties that will access the data, for which reasons, what data points they used, the target audience, and who paid for the ads campaigns.

This type of financial accountability, full transparency regarding the amount spent by companies on ads, also applies to political campaigns sponsorship. Ad political campaigns, which on the internet were often overlooked, would now have their layer of anonymity removed. Yet again removing black propaganda and state-linked accounts from the equation and making microtargeting less obvious.

Many legislatures, regions, states, governments, authorities, and countries have erected or proposed laws to tackle the things we've seen, let's mention some of them.

Related to the financial accountability, the *Honest Ads Act*, is a bill in the USA that was proposed such that online services would be required to reveal the description of the target audience of ads campaigns.

However, this bill wasn't passed yet in favor of self-regulation. The USA, in general, is a laggard on the domain of privacy as it feels more threatened by the intervention of the state than the market.

Still, in 2018, the California Consumer Privacy Protection, a legislature passed in California (a USA state) would guarantee users in that region the right to know what data is being collected, and opting out of the sale of their data.

This opt-out approach isn't the best but it's a start.

Others might find that there needs to be a stronger data protection, that it's part of human dignity and that it shouldn't be threatened by any kind of intrusions. In that view, privacy and ownership over our private data is a default and not an opt-out.

The European Union was the first in 2016 to spear-head this change by rolling out the largest attempt at protecting user data with the *General Data Protection Regulation*.

Privacy laws are not new, for example France's data protection law dates back to 1978, and the EU already had *Data Protection Directive* law about the protection of fundamental rights and freedoms in the processing of personal data, dating from 1995. However, the GDPR is an extension of all this with modernization, clarification, and making it actionable. It is a move that has spurred other states to enforce similar laws. It also gives them more confidence in intervening against the internet behemoths, which they wouldn't dare attack before.

The French data protection law ensures the following rights:

Personal data must be collected and processed fairly and lawfully for

specified, explicit, and legitimate purposes, and with the consent of the data subject. In addition to the right to consent, data subjects have been given the following rights: right to be informed, right to object, right of access, right to correct and delete information, and right to be forgotten.

These have been mapped unto GDPR to hold data processors accountable when manipulating data that isn't mandatory for the functioning of the service. It defines clearly what is meant by personal data, what it means to process it, and what is required of organizations and entities that process it.

The organizations are expected to have a management procedure in place to keep the data safe and secure from breach. That means specific roles need to be in place, such as a Data Protection Officer, and the risk management assured. They are held accountable for the privacy and protection of the data, and data protection assessment can be performed to ensure this is properly applied.

The data subjects keep their rights over their data. They should be informed about the processing activities taking place, the data not being used for any non-legitimate purpose. Their explicit consent needs to be requested for its usage and collection. That means the data subjects have the right to update/correct and erase their data. Additionally, the data subject can ask to see which data is held about them and control whether its transfer can happen between third parties or not.

Most importantly, regulators can ask for demonstrations of accountability and impose fines for the entities that aren't complying. This is the clause that makes the difference with any previous laws.

After it was passed, the internet has been shaken. Most websites have chosen to display annoying pop-ups/notification banners asking if users want to allow their information to be shared with third parties. It defaults to no but it is sometimes hard to manipulate and very intrusive.

Moreover, some companies are also allowing their users residing in the EU to download the personal data that has been gathered, and give them the possibility to delist it, essentially erasing it.

The way the GDPR has been applied by companies has given rise to more dark patterns, persuasive technologies trying to trick users into accepting to give their personal info.

Research has shown that only around 11.8% of consent forms in 2019 met the minimal requirements based on the European law.

Multiple countries have their own privacy laws and acts, and many today are modernizing and reforming them to add actionability like GDPR.

Some even include the right to data portability and the right to object to marketing, the right of non-reception which we mentioned earlier.

Let's take some examples.

Canada has the Privacy Act from 1983, which it is modernizing to be similar to the GDPR in the Personal Information Protection and Electronic Data Act.

China's Personal Information Security Specification that took effect in 2018, and ratified in 2020 in the Personal Information Protection Law, has more strenuous and far-reaching requirements than GDPR applying to any personal data and not only sensitive personal data. The UK has its UK Data Protection Act from 1998, which has been updated in 2018 to follow and supplement the GDPR, and is being updated today to follow its own standards. The Irish Data Protection Commissioner (DPC) upholds the same fundamental privacy standards as the EU. Similarly, Australia has updated its 1988 Privacy Act and Australian Privacy Principles to be like the GDPR. Russia Federal Law on Personal Data of 2006 regulates data processors to protect the defined sensitive personal data against unlawful and accidental access. India's PDP Bill of 2019 goes in the same direction as GDPR but is more integrated with Aadhaar portability which we'll see in a bit. Argentina is going the same way, currently amending their laws to be like the GDPR. etc..

It's apparent that most of the world is moving in the direction of edifying laws to protect the privacy of the citizen from the private corporate data brokers. Market regulations aren't seen as enough.

Some nations take it a step further, considering the protection, privacy, standardization, digitalization, and usage of identity to be the role of the state and not corporations. The state should have a monopoly on identity, just like it should, in theory, have a monopoly on violence because it has the same destructive power.

As we said, sociality requires giving up a bit of privacy, and the digitalization of identity is a requirement for the information society. Some people are uncomfortable with the idea of making it the job of the state and would rather have centralized private entities do that. Yet we know that corporate incentives are only for-profit and not the shared good, which could hinder the transformation of the society into this new era.

Thus, some governments force the private sector to strictly follow their privacy rules, while the public sector uses identity as a utility, a part of public infrastructure for the public services.

This requires standardization, definition, transparency, and data portability of digital identity. We'll come back to this in a bit but first let's imagine social media as one of these services.

We already discussed social media as utilities in the social media section of part 1. We said back then that for it to be a utility, it should change from a want to a need, an essential infrastructure, a necessity like electricity.

Social media could be said to be an integral part of information society, in order to adequately take part in the 21st century as an individual, and thus would be important to have the government provide it to remove any profit incentives from it.

Some believe that current popular social media already act, feel, and are considered by people like utilities. So they push forward the idea of making them as such, just like the telecom sector or electricity sector: a public service

that is regulated by the government.

It would make it easier to ensure the protection of the constitutional rights of users, such as freedom of speech in some countries. Additionally, the government could enforce search neutrality, modeled after net neutrality regulations — essentially assure equal access for everyone.

Yet, others argue that making social media similar to telecom regulations would be bad for the market, reduce innovation and growth because of the lack of competition. This is a market view of the subject.

Moreover, it can be said that social media haven't gained the status of utility because countries don't go haywire when they go down, that there is always an alternative, they are still new and replaced every couple of years.

Furthermore, from the neoliberal perspective, one that dreads authorities and prefers seeing things as a free flowing market, not catching nuances, this is the equivalent of the chilling rise of "*authoritarianism*" and "*fascism*". Words that are used as emphasis to display the attack they feel towards their world view. Still, there might indeed be a new kind of social cooling taking place when we become owners of our social media, instead of having them as private companies. State actors were already requesting personal data from these companies and using them for their gain, as we've seen before. Making them public utilities would instead force the general public to keep it in check, as it would be something they would be indirectly paying to keep running.

Another trend is the one of the digitalization of identity by governments. This is the standardization of identification and identity systems and management that become part of the public infrastructure.

In practice, this is more of a re-definition of national identity cards by making them digital, interoperable, and accessible by all citizens. Having it as an infrastructure means that all kinds of public and private services can rely on it to verify reliably the identity of people.

This comes with a lot of challenges for governments as they have to set in place the legal framework around the infrastructure, its usage, regulations, auditability, traceability, transparency, and obviously actually create a technology that is secure, confidential, keeps the integrity, is scalable, and respectful of all individuals.

The capability of the identity system needs to be well-defined, from authentication, authorization, roles, and delegations available. Some government bodies and international standards have been created for these identity management systems such as ISO, the EU eIDAS, European Self-Sovereign Identity Framework, European Blockchain Services Infrastructure (EBSI), and the GSMA Identity programme and Mobile Connect.

Like with social media as a utility, this comes with the same perception from those who'd rather be surveilled by private companies than their government. But with enough transparency and preparation, the most digitally-skeptic can get on board, especially if the solutions are free and open source as we'll see in the next section.

So far, the implementations of digital identities by governments have only been applied when it comes to accessing public services and KYC processes when signing up for services such as telcos, energy, and banks.

Estonia, India, and China are countries that are leading the way. The upside is convenience and an economic boost. According to McKinsey Global Institute, countries that implement a digital ID scheme can boost their gross domestic product by 3 to 13 percent by 2030.

Estonia has been rolling its digital identity program for the past 20 years. Technically, it is a mandatory 11-digit unique identifier assigned to all citizens above the age of 15 that is stored along with a public-private key pair in a PKI (Public-Key Infrastructure).

The default format of this digital ID is a physical card, an i-card, similar to a credit card, passports, and sim cards: an embedded chip (UICC) protected by PIN codes. Internally these circuit cards use secure elements (SE) as a root of trust to store the sensitive information. We generally refer to this type of technology as hardware security modules (HSM). Other formats exist such as a mobile application that inspired China's version of it, I am not currently aware if the Chinese solution additionally requires an UICC to be inserted in the phones.

The data is stored in a decentralized blockchain that is scalable and secure. Protected against cyber threats, which they've been subject to in the past, and are obviously continuously facing and tackling newer security challenges. Additionally, the data is also backed up in Estonia's e-embassy in Luxembourg.

Practically, this allows someone to be verified during a KYC process (Know Your Customer), login to private or public services, to encrypt or decrypt files securely, and to legally digitally sign documents.

Note that e-signatures are allowed in the EU, through the eSignature Directive, to replace handwritten ones.

Users of such system are thus in the center, practicing self-sovereign identity (SSI), personal autonomy, in full control of who has access to their data. The system allows for traceability and auditability. Citizens can transparently see what data is collected about them, when, why, who has accessed to them, revoke or keep this information, and more. That is unless law enforcement requests access, but they'll still be notified once the investigation wraps up.

This can be abused but the country has shown a strong legal stance whenever law enforcement or doctors took advantage of their positions. The traceability of each access also makes it harder for someone to touch the data without anyone else noticing — unlike traditional physical cabinet storages. This enables more privacy and empowerment than when a private company has control over personal data.

The advantages are obvious: designers of systems save time by relying on the government infrastructure, and citizens too by carrying their life activities online.

This includes banking, e-residency, accessing health records, medical prescrip-

tions, voting, paying taxes, and more. One thing they are considering integrating is their own cryptocurrency.

Estonia also teaches cyber hygiene in elementary school. Education is an important factor that we'll dive into next.

The EU is considering implementing a similar system, but leaving each national authority the choice. However, it is still being discussed and argued if it should be mandated across all nations. They have agreed on eSignature Directive, allowing electronic signatures to be the equivalent of handwritten ones, and took a few steps with encouraging national digital IDs in 2018 through the Electronic Identification And Trust Services (eIDAS) regulation. The implementation of digital ID in Europe would allow cross-border electronic transactions and electronic signatures, but only 14 out of 27 member countries have introduced online authentication systems, such as DigiD in the Netherlands, Belgium's eID card, and Spain's DNIe.

Another large implementation of digital identity is India's Aadhaar. Technically, it is a non-compulsory 12-digit unique identifier, termed Aadhaar, that also comes with a public-private key infrastructure that stores biometric information.

Due to the non-mandatory nature, the government has to ensure that no service can be denied if the person hasn't signed up for Aadhaar. However, in practice, many services are now using it for KYC as a replacement for paper proof of identification.

Moreover, because it isn't mandatory, Aadhaar isn't a proof of citizenship or residence: it doesn't replace other IDs like passports or driver's licenses.

Aadhaar practical form is as a biometric ID system, allowing citizens to prove their identity by simply providing a fingerprint or iris scan for example. There is also an ID card that can be issued.

On top of Aadhaar, the government has rolled out a Unified Payment Interface (UPI) allowing banks to interoperate with Aadhaar. UPI is designed to make person-to-person (p2p) and e-commerce transactions swifter and easier.

For India, this has been a game changer, enabling access to bank accounts and services that most couldn't access before, making them more inclusive. Figures are not robust, but it can be assured that most (4 out of 5) Indian citizens have the ID card.

This saves a lot of overhead, someone can transfer money simply by showing their Aadhaar card, or paying with their fingerprint.

Unfortunately, there are a lot of criticism, calling it a "tech-solutionism" and saying the roll-out has been discriminatory.

Besides, there have been emerging reports regarding the security concerns of the personal data associated with Aadhaar ID being sold in alternate markets.

These flaws in privacy and security need to be addressed with accountability, traceability, and a strong legal framework, similar to what Estonia is doing. So far, Aadhaar doesn't yet seem to put the person in control of their own

information, self-sovereign identity. Plus, the document could be upgraded to be considered a true proof of citizenship.

Additionally, only basic biometrics is not enough, but adding a smart card with a pin to the mix was the way to go. It fulfills: something you know, something you have, something you are.

The development possibilities are there and the outcomes would be interesting.

China has slowly been pushing for its virtual/electronic ID card, a digital ID. Practically, it is a valid national ID that contains biometric information such as face and fingerprints.

The solution takes a mobile-first approach, as an app with QR codes, and would integrate well with all services, both online and offline. It is still in its pilot/trial phase, but would be a true replacement for official ID cards and could be used within popular applications such as WeChat and Alipay. For example, WeChat Payment is already extremely popular for making digital payments.

China's implementation would be directly inspired by Estonia's one, very similar. At China's scale, like India, it would open a lot of future possibilities as 67 percent of Chinese residents do not currently have a credit record. The system would also be linked to a generic credit score database.

China is also eyeing entering the digitalization of the supply chain. Their Standardization Administration describes it neatly: *"First-class companies do standards. Second-tier companies do technology. Third-tier companies do products."*

This means being able to associate identity and traceability of all the supply chain and trade processes across multiple geographies and organizations. A true verifiable life-cycle where you could identify compliance and transparency. For that, they've partnered with international standard organizations such as ISO and ITU, and started designing and implementing the next wave of standardization in cyber-physical trade with its ambitious China 2035 Standards strategy. This initiative is also driven by other organizations such as UN/CEFACT, the ICC, World Customs Organization, the European Union Intellectual Property Office (EUIPO), and International Air Transport Association (IATA).

This type of digital meta-platform, this platform-of-platforms, would empower individual actors by giving them the power of traceability and identity for supply chain and trade. This applies to both people within it and outside it. For the consumer, that would mean being able to reliably see the origin of a product, including its materials, legal, geographical, intellectual-property, its origins, and more. This is essential for many of us, and would make it easy to see the quality of intangible goods.

Consumers, governments, and companies are demanding details about the systems, enterprises, and sources that delivered and transformed the goods along their value chain. They worry most about quality, safety, ethics, and environmental impact, to name

just a few.

This would ensure the transparency when buying products from big platforms that contain sub-markets such as Alibaba, Amazon, and Wal-Mart. This adds a lot of trust and transparency with consumers, they can verify the digital twin of their physical good, along with its history.

Now, that is going digital!

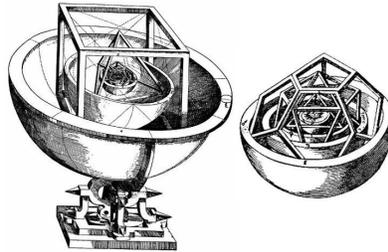
A path towards societal digitalization through internet technologies.

Other countries such as Argentina, Afghanistan, Denmark, Pakistan, Kazakhstan, and more have or are introducing national ID cards with embedded chips used for services and are considering or in the progress of integrating with biometrics, payment, and the online world just like Estonia, India, and China are doing.

This seems like a global trend and is expected to increase with new types of root of trust that can be shared over the wire such as IoT SAFE.

This concludes our review of how governments can bring back order, morals, and ethics on the internet. In a first place, we've dabbled with how the market isn't enough and how there's a need for laws that would consider privacy as a human rights. Then we've seen the balance between sociality and privacy, to whom we'd prefer giving it. Next we went over three topics applied to legality: consent, accountability, and transparency. After that we've looked at some examples, how the world is moving in that direction. Finally, we've tackled identity and social media as utilities and infrastructures, and what that would imply, along with some of today's examples.

## Technical Solutions, Wars and Patches



J. Kepler, *Mysterium Cosmographicum*, 1609

- Detection and Remedial, War of Algorithms
- Changing the Way the Platform Work, Communication and Filters
- Differential Privacy and Privacy First Internet
- Defensive Tools
- Attention Management
- Decentralization, Transparency, and Free Software

When free market and regulations fail, when the laws of rights can't properly protect anyone and trust has eroded, we're left only with ourselves. In that scenario, tech is seen as the savior of the internet, the weapon and armor of choice for everyone, building and selecting software that resolve issues.

For social media platforms and other big entities such as governments, algorithms can be used for detection, categorization, and remedial. The first step of an issue is to know: without knowledge it's hard to defend.

Platforms could employ algorithms that would automatically flag posts containing hate-speech or other sensitive content, and either remove them or let a person take further actions from there. There could also be automatic detection systems that would find bot accounts, satiric content (including deep fake), and state-linked accounts, then label them as such. As we said earlier, if there are laws to tag such accounts, it makes their activities transparent and reduces the chances of black propaganda.

Some even talk of contextualization engines that could bring up the context behind any piece of media posted.

Facebook has recently been experimenting with labeling bot accounts, adding an official stamp on state related and celebrity accounts, and labeling satiric and other types of posts as such. Other platforms are applying comparable labeling, at least for official accounts.

Algorithms could then be countered with algorithms. After detecting malicious intents some actors — be it the platforms to protect their own policies, or states

entities — could launch offensive “*pro-social*” bots themselves, or other means of automatic counter-propaganda as a defense.

However, algorithmic solutions are problematic because they create an arms race. Moreover, the over-reliance on algorithms can have consequential results as they can be reflective of inner-biases. We’ve seen that before.

Another technical solution, in between internet platforms and their users, could be to change criteria that make the internet what it is: speed, exposure, and long-lasting.

There has been some arguable success with platforms that make messages ephemeral, for example. However, these are hard to control because these are innate attributes of the medium.

Rethinking the current way we communicate online and providing means to better communicate without toxicity, filter bubbles, addiction, and extremism is what a lot of people are thinking about today. It’s a question that remains unanswered.

Some have attempted to create platforms around, not only communicating, but also organizing ideas, increasing the efforts to partake in the activities, adding a positive creative gatekeeping.

Some have played with new recommendation algorithms that would increase cognitive diversity, pushing people out of filter bubbles by exposing them to different ideas, cultures, geographies, and anything unfamiliar.

Others are trying to build systems that would be able to put metrics on our biases, on our tendencies to associate with similar people, of clustering. Essentially, creating a self-monitoring to add serendipity, inclusiveness, and diversity in our own lives.

Some have tried a topic-based internet where people are randomly connected based on common interests, instead of vote metrics and shock-value.

Another way is to not put all the facets of our lives in the same place, to distinguish between different activities, hobbies, and interests, to keep them separate. This helps avoid social cooling and facades.

Others are trying to see if the micro-transactions and micro-payments we discussed in a previous section, would work to make an internet of the passion economy and drive away other incentives, leaving only pure human creativity and interests.

Technologically, internet giants are trying to win back the trust of the netizens by talking of differential privacy and privacy first tech.

Like we said before, this is similar to privacy as a product, privacy as market value. However, big techs are selling these words not only for the users but to protect themselves from the law.

Some of these companies are now disabling third-party cookies by default in their products, notifying users of tracking, providing privacy sandboxes, enabling end-to-end and other types of encryptions by default, using differential privacy or cohort-based analysis or context-based ads instead of micro-targeting.

Yet, these all make no sense without transparency and when these entities are

for-profit.

Digital citizens still don't trust them and would rather rely on defensive tools and products to feel safer online and avoid being tracked.

They use tools such as VPN, which we discussed earlier, proxies, and ad blockers. According to statistics 47% of USA internet users now utilize ad blocking software.

Additionally, many are now using attention management and informational management tools to get back the control over their attention. We've seen earlier how the internet can affect us long-term cognitively and how we are inundated with information.

Attention management tools are software that are used to warn people when they get inadvertently absorbed into activities or media. To be proactive instead of reactive.

Informational management tools are database systems used to organize in a clear and concise way the information we find important. They help to deliberately decide what should be in our memory extension, which we discussed when we saw the cognitive changes the internet brings.

One great thing about the internet, is that even though it's convenient, people don't have to use pre-existing platforms, they can be empowered to create their own.

The edification of standards that allow for decentralization and keeping platforms open are good technological ways to avoid bait-and-switch tactics, data leaks, privacy concerns, loss of access, being locked out of accounts, etc..

Avoiding monoliths is avoiding putting all eggs in one basket. Users can choose to spread their internet usage across different services and favor decentralized ones.

On top of this, if netizens have enough patience, expertise, and time, one of the best solution is to own the data and tools by hosting them, self-hosting. This is more than having backup copies of the digital assets, it's also about regaining control, trust, and privacy.

This is what some popular YouTubers and others are doing by building their own site, to not be victims of the market and keep platforms decentralized and open.

Sometimes openness isn't enough, we can host services ourselves but if the software is proprietary then we might still not trust it. What is needed in that case is transparency.

Transparency can be achieved in different ways, self-sovereign identity is one that we've seen in the previous section.

Another way is to use so-called "zero-data" applications, software that let us be in control of our data from the start, doesn't access it, or doesn't do any type of tracking.

Users can rely on feedbacks and recommendations from non-profit organizations that try to defend digital privacy such as the Electronic Frontier Foundation

(EFF) to be up-to-date with the best practices and events in the online sphere. We'll tackle the education part in the next section.

Yet, that can be limiting and not transparent enough. The most transparency we can have from software is when it is open source and when the licenses enforce the respect of freedom and liberty, what we call free software.

Certain non-profit organizations and projects have as mission to promote such kind of user freedom, namely the Free Software Foundation (FSF) and the GNU Project.

Technically savvy netizens could still rely on their own instinct and replace their tools and services with the open sources projects they deem deserve more trust.

Open source and free software licenses can enhance and create value for the public sector too. They can be used within the ICT framework in infrastructure and services offered by the institutions, all publicly funded developments.

Through the use of free software, the citizens and government will feel more in control over information technology. It would grant them digital independence, sovereignty, and security ensuring that citizen's data is handled in a trustworthy manner.

The use of free formats and protocol will also influence the way development is done, increase trust and reduce distance between government software and the citizen involvement. Open source is collaborative and encourages collaboration by nature.

Having everything done in the open, open access (OA), would also reduce waste, avoiding non-replaceable software, and offering technological neutrality. This reminds us of the current trendy discussion rotating around the subject of electronic right to repair.

These could be applied to any government services, especially if they involve social media as a utility and digital identity. The possibilities are interesting.

Practically, this can be implemented at the state or institution level either through the legal system, regulations, policies, or encouragements or promotion (or non-encouragement).

Multiple nation-wide entities and bodies are transitioning to open source or free-software solutions through different measures. For example:

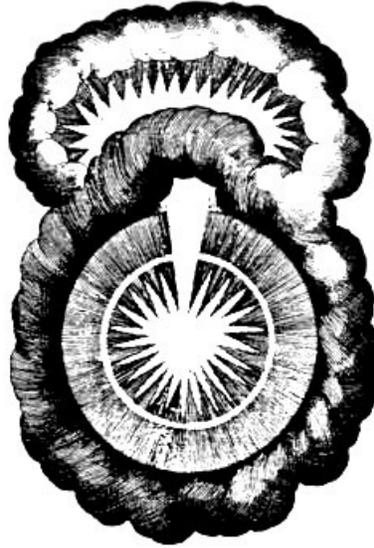
- In 2002, the Peruvian government voted the adoption of open source across all its bodies to ensure the pillars of democracy were safeguarded.
- In 2004, the Venezuelan government passed a law, decree 3390, that would also transition the public agencies to use open source software.
- The National Resource Centre for Free and Open Source Software (NRC-FOSS) in India since 2005 is promoting the use and development of free software.
- The Malaysian Public Sector Open Source Software Program in Malaysia since 2008 is similarly discouraging the use of proprietary-software and encouraging free software.

- In the same year, 2008, Ecuador passed a law, decree 1014, to migrate the public sector to Libre software.
- New-Zealand, in 2010, through its open access initiative, NZGOAL, started promoting the use of free and open source licenses as a guidance for releasing publicly funded software.
- In the same spirit, the UK Government Digital Service formed in 2011 after a proposal from 2010, included in its guideline the promotion of open source when it fits the government IT strategy.

... And countless other examples that show how government entities are promoting or using open source and free software to bring back trust and transparency. As we said earlier, this is a must during the trust and truth crises we are facing.

This concludes our review of technical and software solutions that can be used to avoid issues we've seen such as filter bubbles, toxicity, truth and trust crises, attention and information management, and others. In a first time, we've seen how big entities can use algorithms to fight online content through detection and remedial, either removal or tagging/labeling of content. However, we've also seen that this would give rise to an arms race of bots. Then we've looked at ways internet platforms could change their approach to make communication less toxic and increase cognitive diversity. Next, we've mentioned how internet giants are patching themselves by introducing more privacy and security features in their products. After that, we've said netizens would still lack trust because of the lack of transparency, thus would rely on defensive privacy tools such as VPN, proxies, and ad blockers. Users could also use software tools to help them manage their attention and information. Lastly, we've explored finding transparency and trust by decentralizing services and the usage of free and open source software. This can also be applied at the national level to tackle the trust issue with governments.

## Education, Literacy, and Reality



Origin of the 'Primum Mobile', from: Robert Fludd, *Philosophia Sacra*, Frankfurt, 1626

- Web and Internet Literacy
- Biases and Human Nature
- Our Online Social Lives
- Disconnecting to Better Reconnect
- Learning to Live in the Information Era

We can attempt to patch things, use tools and software as countermeasures, to add laws and regulations, or to let the market decide, but in the end we are at the center of everything. If we are facing difficulties with the medium it's because we haven't matured enough to handle it properly. Right now we're still in the process of trying to grasp how it works, in an apprenticeship stage.

Knowing our tools, how to use the internet medium properly, is a foundational skill, as important as any other in our information society. This goes under the name of digital, internet, or web literacy: the ability to read, write, and participate properly on the medium, in its full extent. It's an application of the broader information literacy.

Literacy is important because it shapes societies. The degree of literacy of people affects directly what they're able to imagine doing and actually do on a medium. By providing these skills to more people, teaching them how to use

the internet, it would make the access to participation more equitable. It would ensure that there would be more representation of diverse ideas, geographies, languages, and cultures. Consequently, it would reduce the digital divide and increase the cognitive diversity of the netizens.

At the moment, as we've seen before, some topics are reserved to the elites. For example, we've dived into privacy as a luxury in one of the previous sections. Bringing internet-literacy to everyone, as a human right, would bridge the class gaps.

In 2016 the UN started considering the right to connect as a human right and some countries have adopted it in their laws. However, education on how to use the medium is as important but often dismissed.

Different organizations have thought this through and came up with pedagogical curriculums for the digital literacy core skills needed.

These are skills that are part of information literacy in general but applied to the internet medium. They fall in these categories:

- Seeking information
- Verifying information
- Using information
- Collaborating and participating
- Ethics
- Security and protection

The Mozilla foundation has created a web literacy curriculum that sets the base for the creation of courses that educators can give. They have three broad sections: write, read, and participate. These are subdivided into particular digital skills such as: designing, coding, composing, revising, remixing, connecting, protecting, open practices, contributing, sharing, evaluating, synthesizing, navigating, and searching.

Instead of jumping without knowing — letting users discover everything by themselves — this curriculum could be taught in schools, or as part of trainings easily available to everyone willing to learn.

Such digital citizenship curriculum would help everyone navigate the internet effectively, communicate on it using a variety of methods and tools to a range of different audiences, and have the adequate critical thinking to be able to evaluate information and arguments, identify patterns and connections, and construct meaningful knowledge that can be applied online and in the real world.

Additionally, this curriculum could have an emphasis on understanding the dynamics of the environment, namely: the actors, economies, and algorithms we've seen throughout the sections.

Awareness is key to empower us against the influential algorithms, the curation engines of the internet, so that we can use them to our advantage.

Inherently part of this dynamic are the last point above of security and protection, which rhyme with anonymity, lack of trust, and the truth crisis we've seen

before.

Security also goes along with privacy, implying tackling social cooling problems. Teaching people about cyberbullying, digital footprints, e-safety, and cyber hygiene as soon as possible is a must to protect ourselves online. As we said, people can, after getting a basic overview of the topics, follow recommendations and news from the Electronic Frontier Foundation (EFF) and other non-profit organizations.

One of the most important aspect of information literacy on the internet is making sure of the veracity of what we are consuming. Some organizations and institutions related to libraries, scholars, and media literacy as a whole have put forward good practices that can be taught to everyone to critically assess and navigate the internet space.

The IFLA (International Federation of Library Associations and Institutions) has redacted a document on how to spot fake news and published it initially on factcheck.org, to later translate it into 45 languages for accessibility.

Similarly, the Center For Media Literacy has also put forward key questions to ask every time we encounter dubious messages.

A critical part of fact checking is to know our own biases, to understand our own vulnerabilities.

Being aware of the existence and inner workings of the techniques that can be used to abuse our biases is the best defence against them. It provides the basis to quickly notice when we're being tricked by messages and take some distance. Be it propaganda or marketing schemes, an intimate knowledge of our automatic impulses, training to be primed to know the coercive nature of these messages, make us proactive instead of reactive.

Outrage and shock are two emotional reactions that are employed to get us caught in the tornado of rampage. Noticing how anger doesn't make our opinion valid, nor more righteous, is essential. Our emotions and opinions shouldn't always mix.

Many of these biases are temporal and only work for a short period of time, this is why they often seek immediacy, scarcity, and speed. Slowing down media sharing and consumption practices is a good method to avoid falling for them. The slow thinking way of processing information, compared with fast thinking, would also counter the speed property of the internet medium.

The author Hans Rosling has written about the declinism mindset, how the media change our perceptions, and how to fight these biases in his book *Factfulness*. The book takes three sides: realization that we do not see the world as is, awareness and identification of our instincts, and how to fight and control them by changing the way we see things.

Documents and teaching materials for educators can be found on the gapminder's website.

Biases and instincts are short-term, on the long-term we should consider habits related to our surroundings, how we participate online and create communities.

Just like it's essential to learn the dynamics of the environment, it's also essential to understand and learn how social interactions work on the internet.

This includes grasping what social biases we are prone to — the influence of our virtual surroundings — a good calibration of what this surrounding consists of, and how they are linked.

To calibrate, we can deliberately determine and examine the gatekeeping level of the community we are part of, or the ones we intend on joining or creating. This can be used to bring back a certain quality and trust.

The calibration can come in the form of segregation or separation of our online interactions and profiles. Instead of partaking on platforms that force us to integrate all of our lives, we have to select the ones that help us distinguish between the multiple facets and activities we do.

In the real world we go to different places with different people to do different things, we can do the same virtually. This would help mitigate the phenomena of private life becoming public life, social cooling, and overall paralysis.

The influence of our digital surrounding comes from various sides, all of them wanting to put us in a box, as a well-defined templated individual. This could be because of marketing, the recommendation and curation engines, or simply the influencers and people we keep up-to-date with.

As with most of what we've mentioned so far, knowledge is the best way to avoid being manipulated to fit a narrative. We could train ourselves in metamemetics thinking to be able to recognize the content of the memplexes, take some distance to criticise them. This would include stopping seeing memes as infotainment and to see them in their real light.

Above all, we need to learn to separate our definition of self from what we consume and share.

We could take this further and distance ourselves completely, to disconnect as a way of reconnecting.

Many are seeking interactions on the internet as an escapism from the difficulties of their lives. To feel safe between the walls of filter bubbles.

Some of these malaises emerge from the cultural insecurities and lacuna we've dived into in other sections.

Yet, some studies have found that these insecurities are reduced, along with fewer biases and reaction to outrage, and better communication, when we pull the plug for a while to do offline activities.

In particular, the most effective studies have looked at performing offline pro-social activities such as helping NGOs. Keep in mind that this should be sustained long enough so that it isn't linked to any online social justice, mob-justice, internet karma points, or the virtual signalling we discussed earlier.

On one side, it works because we get far away from outrage and the negativity that is prominent online. It brings a more positive balance to what we feel

instead of being consumed by our screens and their constantly urgent and pressing issues that we sense we are forced to react to.

On another side, it works because it takes us back to raw reality, with its sense of community away from neoliberalism and individualism. Maybe it shows how real human connection cannot be replicated online, but only the chemical reactions.

Nearly everything distinctive about human nature can be seen as a form of cooperation, and taking part in offline activities brings back our humanity.

Ironically, this is the same mechanism that is used to deprogram people from cults or addictive habits. To create a support group around them, with real connection, bonding, support, and orientation.

It could also be because taking time offline and doing non-profit work changes our neoliberal views, if our societies are inundated with them. We can think again of society as an organism which we are part of, with its flaws, and accepting each member with their minute differences.

This last point is probably what triggers our issues on the internet, the malaise and cultural gaps we talked about but that are not addressed.

Learning to live in the information era and the societies shaped around it needs the acceptance of multi-culturality and ambiguity. It requires a post-modern mindset, or even meta-modern mindset, while most are equipped with a modern one.

For that, we have to make peace with post-modernism and what it implies, without reverting, because of our insecurities, to a cozy pre-modern mindset of tribalism. Some call this transition meta-modernism, or neo-modernism and post-postmodernism.

This means mitigating absolutist thinking, mitigating our inner urge to grasp for reassurances that would reinforce our beliefs when we find ourselves in the absence of certainty. The post-modern world doesn't owe us certainty, on the contrary, it disintegrates absolutisms, annihilate dichotomy thinking (black-and-white mindset), removes categorical imperatives, and all the expectations on oneself and others. For post-modernity and meta-modernity, these are obstacle to our growth, they are our immunity to change and it makes us uncomfortable when we have to let go.

Absolutist thinking can significantly contribute to disorders of mood and affect, which can, in turn, negatively impact our quality of life because the world itself isn't absolute and doesn't bend to our preconceived notions. They are considered cognitive distortions in modern psychology since most of reality and everyday life takes place in the gray area, in between extremes.

This also applies to the trend of over-rationality and over-objectivism, where everything has metrics and is calculated. This over-emphasis on clear definitions and delineations, with no in-betweens, is another kind of absolutist thinking.

Navigating risk and uncertainty is a never ending endeavor. No amount of reassurance will ever quell all of the anxieties we have in

our lifetimes.

This transition from modernity isn't new, it's been happening for almost a hundred years now and is only accelerated by the new attributes the internet brings.

This is clearly seen through some Western and Eastern art movements.

Modernism was about individualism, the conquest of the single person against the world, independence, personal ownership, but also a general malaise about our place in the world, nihilism, existentialism, fordism, seeing humans as tools, consumption, the psychoanalysts such as Freud, and the marketers such as Bernays.

In this transition, initially out of the absurdity of consumption, sprung art movements such as Dada. It had objects at its center and rejected all logic and reasons, the non-sense of all the machineries.

This extended into movements such as surrealism, shinkankakuha, and abstract expressionism that now had in the center the internal human experience and its reflection on the world. It portrayed a space between dreams and reality, using psychic automatism as a tool to extract thoughts, an inner discovery of our own senses and connection with our environment. The Surrealists and the shinkankakuha movement were fascinated by dreams, desire, magic, sexuality, and the revolutionary power of artworks to transform how we understand the world.

All of these movements were prequels to today's post-modernism and meta-modernism. Our malaise was put unto art that expressed our infinite smallness, squeezing out our unconscious thought for us to admire and discover new visions, always reinterpreting, always breaking assumptions.

They express the tension we have between structure and non-structure, in any domain, even vis-à-vis language with topics such semiotics.

Presently, we have neural networks dreaming, algorithms that go into inceptions called deep dreams. We are the spectators of this space, the guides which gets back the reflection of their own dreams through a machine.

Yet, dreams rely on associations, even if unthinkable. They learn from these templated, memplexes, absolutist thinking.

Again, we should learn to distance our definition of self from what we consume, or offered to consume.

To tackle this we have to fix our cultural gaps, to get our act together. Do everything we can to increase our cognitive diversity, to have more global voices, to look for bridge figures, to search for in-betweens be it geographical, ideological, cultural, or others.

We can build internet realities that take into consideration our complexity, our diversity, our various and myriads of ways of expression who and what we are, and how we want to live. To accept the multiple facets of human ingenuity and creativity.

We can deliberately dabble with this way of thinking, this "*meaningness*". The

acceptance of nebulosity and fluidity, to learn to find meaning in uncertainty, to learn inter-sectional, cross-cultural connectivity. We can find our gaps and fix our weaknesses within this space, in others, creating a collage of humanness.

However, this poses multiples forms of challenges to move out of our comfort zones and expand our world views. Societies move the burden on the individuals and ask them to provide the structure and system for themselves instead of delegating it to some absolute authority.

Yet as the meme trickled into other online spaces, the line “we live in a society” – originally intended to be an enlightened statement which denounced the many flaws and contradictions of society – instead turned into a piece of satire.

The online world and discussions that bridge cultures make issues more apparent. These controversial topics need to be addressed openly, not through mobs, but maturely. Each on their own.

Some authors and psychologists have written endlessly on the individual’s effort to make sense of experiences, the meaning-making process, metaperception, neo-perception, and self-transformation.

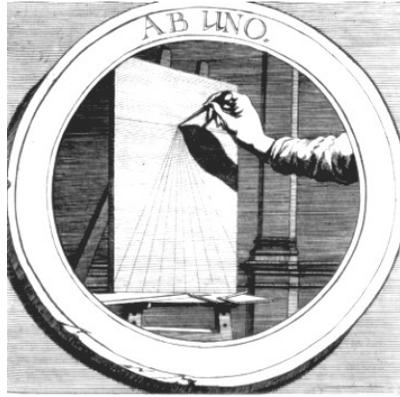
From the “*Mental demands of modern society*” from Kegan, to Piaget subject-object relations, to Erik Erikson “*ego identities*”, to Abraham Maslow “*self-actualization*”.

Learning to live in the informational society is being deliberately open and motivated to possibilities from the intersectionality of all the experiences and ways of seeing the world.

We’re learning to communicate on a global scale while coexisting with algorithms.

This concludes our review of how we can mature to better adapt to the internet medium. We’ve started by exploring educational curriculum such as web and internet literacy, so that we can be properly prepared. We’ve said this includes reading, writing, and participating. Next, we’ve said this curriculum should also take into consideration awareness to biases, knowledge being the best way to tackle them. Later, we’ve mentioned long-term adaptation, social adaptation to the internet, which include learning to manage our connections online by segregating them properly and not being put in templated boxes. After that, we’ve examined completely disconnecting as a way to better reconnect. We’ve seen some studies about helping NGOs and how it reduced biases and our reaction to online outrage. Finally, we’ve dived into what it means to be a netizen of the information era and societies, to live in post-modernity reaching meta-modernity. We’ve discussed some of the artistic transitions and how they reflect our malaise and continuous improvement at including ourselves in this intersectional and cross-cultural world that has never been as connected as today.

## Conclusion



Philotheus, *Symbola Christiana*, Frankfurt, 1677

Our mini internet study has come to an end.

In this book, we've seen the new artifacts and spaces introduced by the internet, the actors using them, from the new economies, to netizens in between, to state actors. We also reflected and tried to understand why we can be susceptible to biases and why we have so many difficulties with online interactions. Next we've looked at the big picture by diving into subjects such as paralysis, neoliberalism, the truth and trust crises, and a future glance at mass hypnosis and psychosis. Finally, in the last part, we've seen four type of solutions: market and economy or laissez-faire, legal path with governments being involved for transparency and accountability, technical software solutions, and web literacy as education and maturity to learn to live in the information society — a post-modern or meta-modern society.

I hope you've learned as much as I did. We've broadly covered quite a lot of topics, from sociology, psychology, computer science, art, memetics, history, warfare studies, politics, and more.

Let me know if it has been as helpful as it has been for me.

# Bibliography

“1% Rule (Internet Culture).” *Wikipedia*, Wikimedia Foundation, 11 Jan. 2021, [https://en.wikipedia.org/wiki/1%25\\_rule\\_\(Internet\\_culture\)](https://en.wikipedia.org/wiki/1%25_rule_(Internet_culture)).

“1957 High School Debate. Nigeria, Ethiopia, Ghana and S.Africa. Subject: Prejudice Part 1.” YouTube, YouTube, 26 Dec. 2020, <https://www.youtube.com/watch?v=840XWjnt9wc>.

David Egts (Lead Contributor) July 23, et al. “4 Myths about Open Source in Government.” The Enterprisers Project, 23 July 2020, <https://enterpriseproject.com/article/2020/7/open-source-government-myths>.

Holmes, Aaron. “533 Million Facebook Users’ Phone Numbers and Personal Data Have Been Leaked Online.” Business Insider, Business Insider, 3 Apr. 2021, <https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4>.

Adam Henderson, et al. “6 Ways Technology Has Changed the Mindset of Modern Employees Forever!” LinkedIn, <https://www.linkedin.com/pulse/6-ways-technology-has-changed-mindset-modern-forever-adam-henderson>.

Tali Gazit, Jenny Bronstein. “Active Participants and Lurkers in Online Discussion Groups: an Exploratory Analysis of Focus Group Interviews and Observation.” Active Participants and Lurkers in Online Discussion Groups: an Exploratory Analysis of Focus Group Interviews, University of Borås, <https://www.informationr.net/ir/23-2/paper791.html>.

A Day in the Life of Your Data, Apple, [https://www.apple.com/privacy/docs/A\\_Day\\_in\\_the\\_Life\\_of\\_Your\\_Data.pdf](https://www.apple.com/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf).

“Adoption of Free and Open-Source Software by Public Institutions.” *Wikipedia*, Wikimedia Foundation, 3 Mar. 2021, [https://en.wikipedia.org/wiki/Adoption\\_of\\_free\\_and\\_open-source\\_software\\_by\\_public\\_institutions](https://en.wikipedia.org/wiki/Adoption_of_free_and_open-source_software_by_public_institutions).

Kokemuller, Neil. “Advertising Models vs. Subscription Models.” Small Business - Chron.com, Chron.com, 26 Oct. 2016, <https://smallbusiness.chron.com/advertising-models-vs-subscription-models-70238.html>.

Whittaker, Zack. “A Huge Database of Facebook Users’ Phone Numbers Found Online.” TechCrunch, TechCrunch, 4 Sept. 2019, <https://techcrunch.com/2019/09/04/facebook-phone-numbers-exposed/>.

“Algorithms, Bots, and Political Communication in the US 2016 Election: The Challenge of Automated Political Communication for Election Law and Administration.” Taylor & Francis, <https://www.tandfonline.com/doi/full/10.1080/19331681.2018.1448735>.

Robb, John. “All Hail the Meme, The New King of Political Communication.” Medium, Medium, 17 Aug. 2016, <https://medium.com/@johnrobb/all-hail-the-mediaglyph-the-king-of-modern-political-communication-26dd2902847d>.

Ko, Amy J. “UW Faculty Web Server.” *Foundations of Information*, <https://faculty.washington.edu/ajko/books/foundations-of-information/>.

“Analysis Paralysis.” *Wikipedia*, Wikimedia Foundation, 8 Apr. 2021, [https://en.wikipedia.org/wiki/Analysis\\_paralysis](https://en.wikipedia.org/wiki/Analysis_paralysis).

Ball, Matthew. “Apple, Its Control Over the iPhone, The Internet, And The Metaverse.” MatthewBall.vc, MatthewBall.vc, 9 Apr. 2021, <https://www.matthewball.vc/all/applemetaverse>.

Miller, Chance, and Chance Miller @ChanceHMiller Chance is an editor for the entire 9to5 network and covers the latest Apple news for 9to5Mac.Tips. “Apple Says App Tracking

- Transparency Feature Will Launch in ‘Early Spring’ with iOS 14 Update.” 9to5Mac, 28 Jan. 2021, <https://9to5mac.com/2021/01/27/app-tracking-transparency-spring/>.
- Jesse Squires. “Apple’s Cooperation with Authoritarian Governments.” Jesse Squires, 30 Mar. 2021, <https://www.jessesquires.com/blog/2021/03/30/apple-cooperation-with-authoritarian-governments/>.
- i-Sight. “A Practical Guide to Data Privacy Laws by Country.”, <https://i-sight.com/resource/s/a-practical-guide-to-data-privacy-laws-by-country/>.
- voxdotcom. “Are We Automating Racism?” YouTube, YouTube, 31 Mar. 2021, <https://www.youtube.com/watch?v=Ok5sKLXqynQ>.
- “Attention Economy.” *Wikipedia*, Wikimedia Foundation, 16 Apr. 2021, [https://en.wikipedia.org/wiki/Attention\\_economy](https://en.wikipedia.org/wiki/Attention_economy).
- “Attention Management.” *Wikipedia*, Wikimedia Foundation, 1 Feb. 2021, [https://en.wikipedia.org/wiki/Attention\\_management](https://en.wikipedia.org/wiki/Attention_management).
- “Australia Passes Law Making Facebook, Google Pay for News”, Bloomberg, <https://www.bloomberg.com/news/articles/2021-02-24/australia-passes-law-forcing-facebook-google-to-pay-for-news>.
- Gwern. “Banner Ads Considered Harmful.” Gwern.net, 8 Jan. 2017, <https://www.gwern.net/Ads>.
- “BBC Internet Blog: BBC Online Briefing Spring 2012: The Participation Choice.” BBC, BBC, [https://www.bbc.co.uk/blogs/bbcinternet/2012/05/bbc\\_online\\_briefing\\_spring\\_201\\_1.html](https://www.bbc.co.uk/blogs/bbcinternet/2012/05/bbc_online_briefing_spring_201_1.html).
- Nosta, John. “Thought As Currency.” Psychology Today, Sussex Publishers, 16 Apr. 2021, <https://www.psychologytoday.com/us/blog/the-digital-self/202104/thought-currency>.
- “Mass Surveillance in the United Kingdom.” *Wikipedia*, Wikimedia Foundation, 5 Apr. 2021, [https://en.wikipedia.org/wiki/Mass\\_surveillance\\_in\\_the\\_United\\_Kingdom](https://en.wikipedia.org/wiki/Mass_surveillance_in_the_United_Kingdom).
- Ferris, Andy, et al. “Big Data What Is It, How Is It Collected and How Might Life Insurers Use It.” The Actuary Magazine (2013): 28-32, <https://www.soa.org/globalassets/assets/Library/Newsletters/The-Actuary-Magazine/2013/december/act-2013-vol10-iss6-srivastava.pdf>.
- “Black Propaganda.” *Wikipedia*, Wikimedia Foundation, 9 Mar. 2021, [https://en.wikipedia.org/wiki/Black\\_propaganda](https://en.wikipedia.org/wiki/Black_propaganda).
- “Booking.com Fined €475,000 for Reporting Data Breach Too Late.” The Record by Recorded Future, 31 Mar. 2021, <https://therecord.media/booking-com-fined-e475000-for-reporting-data-breach-too-late/>.
- Huxley, Aldous. “Brave New World (1932).” London: Vintage (1998).
- “Brave New World.” *Wikipedia*, Wikimedia Foundation, 15 Apr. 2021, [https://en.wikipedia.org/wiki/Brave\\_New\\_World](https://en.wikipedia.org/wiki/Brave_New_World).
- “Bringing It All Together.” Neoliberalism and the Internet, 23 Oct. 2010, <https://anth2128.wordpress.com/2010/10/23/bringing-it-all-together/>.
- Lomas, Natasha. “Cambridge Analytica’s Parent Pleads Guilty to Breaking UK Data Law.” TechCrunch, TechCrunch, 9 Jan. 2019, <https://techcrunch.com/2019/01/09/cambridge-analyticas-parent-pleads-guilty-to-breaking-uk-data-law/>.
- “Cancel Culture.” *Wikipedia*, Wikimedia Foundation, 15 Apr. 2021, [https://en.wikipedia.org/wiki/Cancel\\_culture](https://en.wikipedia.org/wiki/Cancel_culture).
- Five Key Questions of Media Literacy, Center for Media Literacy, 2005. [http://www.medialit.org/sites/default/files/14B\\_CCKQPoster+5essays.pdf](http://www.medialit.org/sites/default/files/14B_CCKQPoster+5essays.pdf)

Kgspencer. "Charles Taylor's The Ethics of Authenticity (Chapters 1-5)." Seoul Philosophy Club, 30 Aug. 2015, <https://seoulphilosophy.wordpress.com/2015/06/19/charles-taylors-the-ethics-of-authenticity-chapters-1-5/>.

laozi200. "The Malaise of Modernity (3/5) - Charles Taylor." YouTube, YouTube, 21 May 2015, [https://www.youtube.com/watch?v=Cxcin\\_pZIRQ](https://www.youtube.com/watch?v=Cxcin_pZIRQ).

Temkin, David. "Charting a Course towards a More Privacy-First Web." Google, Google, 3 Mar. 2021, <https://blog.google/products/ads-commerce/a-more-privacy-first-web/>.

"Citizen Journalism." *Wikipedia*, Wikimedia Foundation, 21 Mar. 2021, [https://en.wikipedia.org/wiki/Citizen\\_journalism](https://en.wikipedia.org/wiki/Citizen_journalism).

"Communication Studies." *Wikipedia*, Wikimedia Foundation, 14 Apr. 2021, [https://en.wikipedia.org/wiki/Communication\\_studies](https://en.wikipedia.org/wiki/Communication_studies).

"Countering Disinformation: Russia's Infowar in Ukraine." The Henry M. Jackson School of International Studies, 15 Mar. 2021, <https://jsis.washington.edu/news/russia-disinformation-ukraine/>.

"Counterpropaganda." *Wikipedia*, Wikimedia Foundation, 22 Dec. 2020, <https://en.wikipedia.org/wiki/Counterpropaganda>.

Patrick Louis aka venam. "Cross Culture Frustration." *Venam's Blog*, Patrick Louis Aka Venam, 4 July 2017, <https://venam.nixers.net/blog/psychology/2017/07/05/culture-frustration.html>.

"Culture War." *Wikipedia*, Wikimedia Foundation, 7 Apr. 2021, [https://en.wikipedia.org/wiki/Culture\\_war](https://en.wikipedia.org/wiki/Culture_war).

"Cyberpolitics." *Wikipedia*, Wikimedia Foundation, 7 Sept. 2020, <https://en.wikipedia.org/wiki/Cyberpolitics>.

Dark Patterns, <https://darkpatterns.org/>.

Nouwens, Midas, et al. "Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence." Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. 2020. <https://dl.acm.org/doi/10.1145/3313831.3376321>

"Dark Pattern." *Wikipedia*, Wikimedia Foundation, 7 Apr. 2021, [https://en.wikipedia.org/wiki/Dark\\_pattern](https://en.wikipedia.org/wiki/Dark_pattern).

"Data Protection Act 2018." *Wikipedia*, Wikimedia Foundation, 8 Apr. 2021, [https://en.wikipedia.org/wiki/Data\\_Protection\\_Act\\_2018](https://en.wikipedia.org/wiki/Data_Protection_Act_2018).

"Data Protection Commissioner." *Wikipedia*, Wikimedia Foundation, 8 Apr. 2021, [https://en.wikipedia.org/wiki/Data\\_Protection\\_Commissioner](https://en.wikipedia.org/wiki/Data_Protection_Commissioner).

Giesea, Jeff. "It's time to embrace memetic warfare." Defence Strategic Communications 1.1 (2015): 67-75, <https://www.stratcomcoe.org/academic-journal-defence-strategic-communications-voll>.

(www.dw.com), Deutsche Welle. "The Democracy of the Gullible: DW: 29.05.2020." DW.COM, <https://www.dw.com/en/the-democracy-of-the-gullible/a-53614771>.

dhcolman. "Despotism 1946." YouTube, YouTube, 22 Nov. 2016, <https://www.youtube.com/watch?v=tIwXdOvEPXE>.

"Different People Use the Internet Differently." Neoliberalism and the Internet, 20 Oct. 2010, <https://anth2128.wordpress.com/2010/10/19/different-people-use-the-internet-differently/>.

"DigiD." *Wikipedia*, Wikimedia Foundation, 12 July 2020, <https://en.wikipedia.org/wiki/DigiD>.

- Zuckerman, Ethan. *Digital cosmopolitans: Why we think the Internet connects us, why it doesn't, and how to rewire it*. WW Norton & Company, 2013.
- Ethan Zuckerman. "Digital Cosmopolitans: Talks at Google." YouTube, 1 Dec. 2014, <https://youtu.be/6sQ9Yhh3wY8>.
- "Digital Identity." *Wikipedia*, Wikimedia Foundation, 16 Apr. 2021, [https://en.wikipedia.org/wiki/Digital\\_identity](https://en.wikipedia.org/wiki/Digital_identity).
- "Digital Identity in China: Today & Tomorrow." <https://Www.trulioo.com>, <https://www.trulioo.com/blog/digital-identity-china>.
- GSMA, World Bank Group, and Security Identity Alliance. *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*. World Bank, 2016, <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf>.
- Promethean. "Digital Literacy in the Classroom. How Important Is It?" Promethean Blog, 1 Apr. 2021, <https://resourced.prometheanworld.com/digital-literacy-classroom-important/>.
- Cjr. "Digital News Consumers Unlikely to Pay for Content and Increasingly Block Ads." *Columbia Journalism Review*, [https://www.cjr.org/analysis/reuters\\_digital\\_news\\_report.php](https://www.cjr.org/analysis/reuters_digital_news_report.php).
- "Disinformation and 'Fake News': Interim Report." *Disinformation and 'Fake News': Interim Report - Digital, Culture, Media and Sport Committee - House of Commons*, <https://publications.parliament.uk/pa/cm201719/cmselect/cmcomeds/363/36303.htm>.
- "DoD Open Source Software (OSS) FAQ." *Open Source Software FAQ*, <https://dodcio.defense.gov/Open-Source-Software-FAQ/>.
- Hancock, Alexis, et al. *Electronic Frontier Foundation*, <https://www.eff.org/>.
- "Electronic Identity Card." *Wikipedia*, Wikimedia Foundation, 6 May 2017, [https://en.wikipedia.org/wiki/Electronic\\_identity\\_card](https://en.wikipedia.org/wiki/Electronic_identity_card).
- "Electronics Right to Repair." *Wikipedia*, Wikimedia Foundation, 30 Mar. 2021, [https://en.wikipedia.org/wiki/Electronics\\_right\\_to\\_repair](https://en.wikipedia.org/wiki/Electronics_right_to_repair).
- Parsovs, Arnis. *Estonian Electronic Identity Card and its Security Challenges*. Diss. PhD thesis (to be completed). University of Tartu, 2020, [https://dspace.ut.ee/bitstream/handle/10062/71481/parsovs\\_arnis.pdf?sequence=1&isAllowed=y](https://dspace.ut.ee/bitstream/handle/10062/71481/parsovs_arnis.pdf?sequence=1&isAllowed=y).
- "Ethical Anti-Design, or Designing Products That People Can't Get Addicted to." *Njms*, <https://njms.ca/posts/ethical-anti-design.html>.
- Bhargava, Vikram R., and Manuel Velasquez. "Ethics of the Attention Economy: The Problem of Social Media Addiction." *Business Ethics Quarterly* (2020): 1-39, <https://www.cambridge.org/core/journals/business-ethics-quarterly/article/ethics-of-the-attention-economy-the-problem-of-social-media-addiction/1CC67609A12E9A912BB8A291FDFFE799>.
- Irrera, Anna. "Exclusive: PayPal Launches Crypto Checkout Service." *Reuters*, Thomson Reuters, 30 Mar. 2021, <https://www.reuters.com/article/us-crypto-currency-paypal-exclusive-idUSKBN2BM10N>.
- Hussain, Noor Zainab. "Exclusive: Visa Moves to Allow Payment Settlements Using Cryptocurrency." *Reuters*, Thomson Reuters, 29 Mar. 2021, <https://www.reuters.com/article/us-crypto-currency-visa-exclusive/exclusive-visa-moves-to-allow-payment-settlements-using-cryptocurrency-idUSKBN2BL0X9>.
- Zakem, Vera, Megan K. McBride, and Kate Hammerberg. *Exploring the utility of memes for US government influence campaigns*. Center for Naval Analyses Arlington United States, 2018, [https://www.cna.org/CNA\\_files/PDF/DRM-2018-U-017433-Final.pdf](https://www.cna.org/CNA_files/PDF/DRM-2018-U-017433-Final.pdf).

Vincent, James. “Facebook Hopes Tiny Labels on Posts Will Stop Users Confusing Satire with Reality.” *The Verge*, The Verge, 8 Apr. 2021, <https://www.theverge.com/2021/4/8/22373291/facebook-label-news-feed-page-posts-fan-satire-public-official>.

“Facebook’s Data-Sharing Deals Exposed.” *BBC News*, BBC, 19 Dec. 2018, <https://www.bbc.com/news/technology-46618582>.

“Facebook’s GDPR Bypass Reaches Austrian Supreme Court.” *Noyb.eu*, 14 Mar. 2021, <https://noyb.eu/en/facebooks-gdpr-bypass-reaches-austrian-supreme-court>.

Moon, Mariella. “Facebook Test Adds Contextual ‘Labels’ to Popular Pages.” *Engadget*, 8 Apr. 2021, <https://www.engadget.com/facebook-experiment-label-pages-090724411.html>.

“Facebook v Apple: the Looming Showdown over Data Tracking and Privacy.” *The Guardian*, Guardian News and Media, 13 Feb. 2021, <https://www.theguardian.com/technology/2021/feb/14/facebook-v-apple-the-looming-showdown-over-data-tracking-and-privacy>.

FactCheck.org, <[www.factcheck.org/](http://www.factcheck.org/)>.

“Factfulness.” *Gapminder*, <https://www.gapminder.org/factfulness/>.

Ahmad, Irfan. “Find Out Where Apple, Facebook, Google, Twitter and Other Tech Giants Are Sending Your Data.” *Digital Information World*, 9 Aug. 2019, <https://www.digitalinformationworld.com/2019/08/find-out-where-facebook-google-apple-airbnb-others-are-sending-your-data.html>.

Flarum, <https://flarum.org/>.

Grothaus, Michael. “Forget the New iPhones: Apple’s Best Product Is Now Privacy.” *Fast Company*, Fast Company, 14 Sept. 2018, <https://www.fastcompany.com/90236195/forget-the-new-iphones-apples-best-product-is-now-privacy>.

DiResta, Renee. “Free Speech Is Not the Same As Free Reach.” *Wired*, Conde Nast, <https://www.wired.com/story/free-speech-is-not-the-same-as-free-reach/>.

Free Software Foundation - Working Together for Free Software, <https://www.fsf.org/>.

Dreamseeker, Soatok. “Gatekeeping in Online Communities.” *Medium*, Medium, 6 Mar. 2021, <https://medium.com/@soatok/gatekeeping-in-online-communities-48dec7f97f6a>.

“An Overview of the General Data Protection Act.” *GDPR Summary*, 6 Dec. 2020, <https://www.gdprsummary.com/gdpr-summary/>.

“General Data Protection Regulation.” *Wikipedia*, Wikimedia Foundation, 12 Apr. 2021, [https://en.wikipedia.org/wiki/General\\_Data\\_Protection\\_Regulation](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation).

*GlobalPlatform Root of Trust*, NIST, [https://csrc.nist.gov/CSRC/media/Presentations/GlobalPlatform-Root-of-Trust/images-media/day2\\_trusted-computing\\_100-150.pdf](https://csrc.nist.gov/CSRC/media/Presentations/GlobalPlatform-Root-of-Trust/images-media/day2_trusted-computing_100-150.pdf).

Glue Comic, <https://a9.io/glue-comic/>.

“The GNU Operating System and the Free Software Movement.” *A GNU Head*, <https://www.gnu.org/>.

Cyphers, Bennett. “Google Is Testing Its Controversial New Ad Targeting Tech in Millions of Browsers. Here’s What We Know.” *Electronic Frontier Foundation*, 9 Apr. 2021, <https://www.eff.org/deeplinks/2021/03/google-testing-its-controversial-new-ad-targeting-tech-millions-browsers-heres>.

Australian Competition and Consumer Commission. “Google Mised Consumers about the Collection and Use of Location Data.” *Australian Competition and Consumer Commission*, 16 Apr. 2021, <https://www.accc.gov.au/media-release/google-mised-consumers-about-the-collection-and-use-of-location-data>.

Ikeda, Scott. "Google Phases Out Use of Apple IDFA as New IOS 14 Ad Tracking Notifications Are Set for Early Spring." *CPO Magazine*, 31 Jan. 2021, <https://www.cpomagazine.com/data-privacy/google-phases-out-use-of-apple-idfa-as-new-ios-14-ad-tracking-notifications-are-set-for-early-spring>.

graham, Megan c. "Google Says It's Confident about Alternatives to Browser Cookies That Track You for Ads." *CNBC*, CNBC, 25 Jan. 2021, <https://www.cnn.com/2021/01/24/google-extremely-confident-about-third-party-cookie-alternatives-.html>.

O'Neill, Patrick Howell. "Google's Unusual Move to Shut down an Active Counterterrorism Operation Being Conducted by a Western Democracy." *MIT Technology Review*, MIT Technology Review, 28 Mar. 2021, <https://www.technologyreview.com/2021/03/26/1021318/google-security-shut-down-counter-terrorist-us-ally/>.

Schechner, Sam, and Keach Hagey. "Google to Stop Selling Ads Based on Your Specific Web Browsing." *The Wall Street Journal*, Dow Jones & Company, 3 Mar. 2021, <https://www.wsj.com/articles/google-to-stop-selling-ads-based-on-your-specific-web-browsing-11614780021>.

GSMA: Identity, 8 Mar. 2021, <https://www.gsma.com/identity/>.

"IoT SAFE." *Internet of Things*, 9 Dec. 2019, <https://www.gsma.com/iot/iot-safe/>.

"Hardware Security Module." *Wikipedia*, Wikimedia Foundation, 21 Feb. 2021, [https://en.wikipedia.org/wiki/Hardware\\_security\\_module](https://en.wikipedia.org/wiki/Hardware_security_module).

"Hashtag Activism." *Wikipedia*, Wikimedia Foundation, 26 Mar. 2021, [https://en.wikipedia.org/wiki/Hashtag\\_activism](https://en.wikipedia.org/wiki/Hashtag_activism).

"The Transparent Supply Chain." *Harvard Business Review*, 7 Sept. 2017, <https://hbr.org/2017/09/the-transparent-supply-chain>.

Patrick Louis aka venam. "Hidden Hope For Control." *Venam's Blog*, Patrick Louis Aka Venam, 27 Oct. 2017, <https://venam.nixers.net/blog/psychology/2017/10/28/will-for-control.html>.

"Hitting the Books: How Biased AI Can Hurt Users or Boost a Business's Bottom Line." *Engadget*, <https://www.engadget.com/hitting-the-books-a-citizens-guide-to-artificial-intelligence-john-zerilli-mit-press-153035570.html>.

"Homophily." *Wikipedia*, Wikimedia Foundation, 9 Feb. 2021, <https://en.wikipedia.org/wiki/Homophily>.

Klobuchar, Amy. "Text - S.1989 - 115th Congress (2017-2018): Honest Ads Act." *Congress.gov*, 26 June 2018, <https://www.congress.gov/bills/115/congress/115th-congress/senate-bills/1989/text>.

Metadium. "How Estonia Is Pioneering the Digital Identity Space." *Medium*, Metadium, 16 July 2019, <https://medium.com/metadium/how-estonia-is-pioneering-the-digital-identity-space-4008c709fbb8>.

Thompson, Stuart A., and Charlie Warzel. "They Used to Post Selfies. Now They're Trying to Reverse the Election." *The New York Times*, The New York Times, 14 Jan. 2021, <https://www.nytimes.com/2021/01/14/opinion/facebook-far-right.html>.

Ascott, Tom, et al. "How Memes Are Becoming the New Frontier of Information Warfare." *The Strategist*, 19 Feb. 2020, <https://www.aspistrategist.org.au/how-memes-are-becoming-the-new-frontier-of-information-warfare/>.

Donovan, Joan. "How Memes Got Weaponized: A Short History." *MIT Technology Review*, MIT Technology Review, 2 Apr. 2020, <https://www.technologyreview.com/2019/10/24/132228/political-war-memes-disinformation/>.

Read, Max. "How Much of the Internet Is Fake?" *Intelligencer*, Intelligencer, 26 Dec. 2018, <https://nymag.com/intelligencer/2018/12/how-much-of-the-internet-is-fake.html>.

- Starr, Paul. "How Neoliberal Policy Shaped the Internet-and What to Do About It Now." *The American Prospect*, 2 Oct. 2019, <https://prospect.org/power/how-neoliberal-policy-shaped-internet-surveillance-monopoly/>.
- "How PR Sold the War in the Persian Gulf." *PR Watch*, 5 June 2013, <https://www.prwatch.org/books/tsigfy10.html>.
- Fumo, Nicola. "The Best MLK Day Furniture Sales To Shop Before They're Over." *Forbes*, Forbes Magazine, 18 Jan. 2021, <https://www.forbes.com/sites/forbes-personal-shopper/2021/01/18/best-mlk-furniture-sales/>.
- Whitler, Kimberly A. "How The Subscription Economy Is Disrupting The Traditional Business Model." *Forbes*, Forbes Magazine, 19 Jan. 2016, <https://www.forbes.com/sites/kimberlywhitler/2016/01/17/a-new-business-trend-shifting-from-a-service-model-to-a-subscription-based-model/>.
- "How to Control People's Thoughts with Words." *Bekindrewrite*, 24 Aug. 2013, <https://bekindrewrite.com/2011/12/10/how-to-control-peoples-thoughts-with-words/>.
- "How to Have Better Arguments Online." *The Guardian*, Guardian News and Media, 16 Feb. 2021, <https://www.theguardian.com/society/2021/feb/16/how-to-have-better-arguments-social-media-politics-conflict>.
- Shukla, Aditya, and Aditya ShuklaHey "How to Overcome Phone Addiction Solutions + Research." *Cognition Today*, 3 Jan. 2021, <https://cognitiontoday.com/phone-addiction-coping-solutions-research-statistics/>.
- "How To Spot Fake News." *IFLA*, <https://www.ifla.org/publications/node/11174>.
- Stauffer, Bri. "How to Teach Digital Literacy Skills." *Digital Curriculum for CTE & Elective Teachers*, <https://www.aeseducation.com/blog/teach-digital-literacy-skills>.
- "How U.S. Media Lost the Trust of the Public" *CBCnews*, CBC/Radio Canada, 28 Mar. 2021, <https://www.cbc.ca/news/world/media-distrust-big-news-1.5965622>.
- Programmer, WeChat Mini. "HOW WILL WECHAT ELECTRONIC ID SYSTEM WORK?" *Medium*, Medium, 24 May 2019, <https://medium.com/@wechatminiprogrammer/how-will-wechat-electronic-id-system-work-26b35f09f83f>.
- Stöcker, Carsten. "Identity in a Multi-Polar World and China's 2035 Standards." *Medium*, Spherity, 6 Jan. 2021, <https://medium.com/spherity/identity-in-a-multi-polar-world-and-chinas-2035-standards-66f14865b800>.
- "Identity Management." *Wikipedia*, Wikimedia Foundation, 14 Apr. 2021, [https://en.wikipedia.org/wiki/Identity\\_management](https://en.wikipedia.org/wiki/Identity_management).
- Wilson, David Sloan. "I Have Come to Bury Ayn Rand - Issue 98: Mind." *Nautilus*, 24 Mar. 2021, <https://nautil.us/issue/98/mind/i-have-come-to-bury-ayn-rand>.
- Trotter, Shane. "I'm Offended: How The Social Justice Warriors Made Thinking Dangerous." *Inspired Human Development*, Inspired Human Development, 18 Nov. 2020, <https://inspiredhumandevlopment.com/blog/social-justice-warriors>.
- "Inceptionism: Going Deeper into Neural Networks." *Google AI Blog*, 17 June 2015, <https://ai.googleblog.com/2015/06/inceptionism-going-deeper-into-neural.html>.
- Robinson, Nathan J. "In Defense Of Social Justice." *Current Affairs*, <https://www.currentaffairs.org/2018/05/in-defense-of-social-justice>.
- Skinner, Chris M. "India's Billion Digital Identities." *Chris Skinner's Blog*, 6 Sept. 2016, <https://thefinanser.com/2016/09/indias-billion-people-digital-identities.html/>.
- "India's New Intermediary Liability and Digital Media Regulations Will Harm the Open Internet." *Open Policy & Advocacy*, 2 Mar. 2021, <https://blog.mozilla.org/netpolicy/2021/03>

/02/indias-new-intermediary-liability-and-digital-media-regulations-will-harm-the-open-internet/.

Klein, Naomi. "India Targets Climate Activists With the Help of Big Tech." *The Intercept*, 27 Feb. 2021, <https://theintercept.com/2021/02/27/india-climate-activists-twitter-google-facebook/>.

Tomoriová, Františka. "Information ethics in the context of information Literacy." *ProInflow* 8.2 (2016), [https://digilib.phil.muni.cz/bitstream/handle/11222.digilib/135937/2\\_ProInflow\\_8-2016-2\\_8.pdf?sequence=1](https://digilib.phil.muni.cz/bitstream/handle/11222.digilib/135937/2_ProInflow_8-2016-2_8.pdf?sequence=1)

"Information Overload." *Wikipedia*, Wikimedia Foundation, 5 Apr. 2021, [https://en.wikipedia.org/wiki/Information\\_overload](https://en.wikipedia.org/wiki/Information_overload).

"Information Pollution." *Wikipedia*, Wikimedia Foundation, 10 Feb. 2021, [https://en.wikipedia.org/wiki/Information\\_pollution](https://en.wikipedia.org/wiki/Information_pollution).

"Information Revolution." *Wikipedia*, Wikimedia Foundation, 7 Dec. 2020, [https://en.wikipedia.org/wiki/Information\\_revolution](https://en.wikipedia.org/wiki/Information_revolution).

"Information Society." *Wikipedia*, Wikimedia Foundation, 9 Feb. 2021, [https://en.wikipedia.org/wiki/Information\\_society](https://en.wikipedia.org/wiki/Information_society).

Kegan, Robert. In over our heads: *The mental demands of modern life*. Harvard University Press, 1994.

"Inside Aadhaar, India's Massive Digital Identity Program." *Tearsheet*, <https://tearsheet.co/data/inside-aadhaar-indias-massive-digital-identity-program/>.

Tom. "Inside a Viral Website." *Not Fun at Parties*, Not Fun at Parties, 31 Mar. 2021, <https://notfunatparties.substack.com/p/inside-a-viral-website>.

"Intellectual Dark Web." *Wikipedia*, Wikimedia Foundation, 15 Apr. 2021, [https://en.wikipedia.org/wiki/Intellectual\\_dark\\_web](https://en.wikipedia.org/wiki/Intellectual_dark_web).

"Internet Culture." *Wikipedia*, Wikimedia Foundation, 29 Mar. 2021, [https://en.wikipedia.org/wiki/Internet\\_culture](https://en.wikipedia.org/wiki/Internet_culture).

Kulkarni, Anushka. "Internet meme and Political Discourse: A study on the impact of internet meme as a tool in communicating political satire." *Journal of Content, Community & Communication Amity School of Communication* 6 (2017), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3501366](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3501366).

"Introduction to Secure Elements" *GlobalPlatform*, <https://globalplatform.org/wp-content/uploads/2018/05/Introduction-to-Secure-Element-15May2018.pdf>.

academyofideas. "Is a Mass Psychosis the Greatest Threat to Humanity?" *YouTube*, YouTube, 26 Feb. 2021, <https://www.youtube.com/watch?v=ojPcF-oLAbE>.

"The Manufacturing of a Mass Psychosis – Can Sanity Return to an Insane World?" *Academy of Ideas | Free Minds for a Free Society*, 24 Apr. 2021, <https://academyofideas.com/2021/04/manufacturing-of-a-mass-psychosis-can-sanity-return-to-an-insane-world/>.

PYMNTS.com. "Is China Roadmap For Digital ID Verification?" *PYMNTS.com*, 18 July 2019, <https://www.pymnts.com/authentication/2019/china-roadmap-red-flag-digital-identity-verification/>.

Heid, Markham. "Is Hypnosis Real? Here's What Science Says." *Time*, Time, 4 Sept. 2018, <https://time.com/5380312/is-hypnosis-real-science/>.

"Is India's Digital ID System, Aadhaar, a Tech Solution for a Socio-Economic Problem?" *Global Voices*, 17 Aug. 2020, <https://globalvoices.org/2020/08/16/is-indias-digital-id-system-aadhaar-a-tech-solution-for-a-socio-economic-problem/>.

- Ryder, John. "Is Total Mind Control Possible?" *Psychology Today*, Sussex Publishers, 24 Sept. 2015, <https://www.psychologytoday.com/us/blog/hypnosis-the-power-trance/201509/is-total-mind-control-possible>.
- "Is Your Government Requesting User Data from Tech Giants?" *AddictiveTips*, 4 May 2020, <https://www.addictivetips.com/news/government-requests-for-user-data-from-tech-giants/>.
- Warzel, Charlie. "It's Not Cancel Culture - It's A Platform Failure.?" *Galaxy Brain*, Galaxy Brain, 13 Apr. 2021, <https://warzel.substack.com/p/its-not-cancel-culture-its-a-platform>.
- Giesea, Jeff. "It's time to embrace memetic warfare." *Defence Strategic Communications 1.1* (2015): 67-75, <https://www.act.nato.int/images/stories/media/doclibrary/open201705-memetic1.pdf>.
- Singer, Natasha. "Just Don't Call It Privacy." *The New York Times*, The New York Times, 22 Sept. 2018, <https://www.nytimes.com/2018/09/22/sunday-review/privacy-hearing-amazon-google.html>.
- "Keeping Track of Your Things." *Nixers*, <https://nixers.net/Thread-Keeping-Track-of-Your-Things>.
- BBF Digital. "KEY DRIVERS OF SUBSCRIPTION-BASED ECONOMY." *BBF Digital*, 3 Oct. 2018, <https://bbf.digital/key-drivers-of-subscription-based-economy>.
- Australian Competition and Consumer Commission. "Lack of Competition in Ad Tech Affecting Publishers, Advertisers and Consumers." *Australian Competition and Consumer Commission*, 28 Jan. 2021, <https://www.accc.gov.au/media-release/lack-of-competition-in-ad-tech-affecting-publishers-advertisers-and-consumers>.
- "La Fabrique De L'ignorance." *IMDb*, IMDb.com, 23 Feb. 2021, <https://www.imdb.com/title/tt14113576/>.
- Paris, R.A.P. "Liberté De Réception." *Résistance à L'Agression Publicitaire*, Résistance à L'Agression Publicitaire, 6 June 2020, <https://antipub.org/glossaire/liberte-de-reception/>.
- "List of Cognitive Biases." *Wikipedia*, Wikimedia Foundation, 15 Apr. 2021, [https://en.wikipedia.org/wiki/List\\_of\\_cognitive\\_biases](https://en.wikipedia.org/wiki/List_of_cognitive_biases).
- "Living Like It's 99: No Social Media, No Smartphone." *Gregory Alvarez*, 19 Feb. 2021, <https://www.alvarez.io/posts/living-like-its99/>.
- "Loot Boxes Linked to Problem Gambling in New Research." *BBC News*, BBC, 2 Apr. 2021, <https://www.bbc.co.uk/news/technology-56614281>.
- "Lurker." *Wikipedia*, Wikimedia Foundation, 20 Jan. 2021, <https://en.wikipedia.org/wiki/Lurker>.
- "Maslow's Hierarchy of Needs." *Wikipedia*, Wikimedia Foundation, 7 Apr. 2021, [https://en.wikipedia.org/wiki/Maslow's\\_hierarchy\\_of\\_needs](https://en.wikipedia.org/wiki/Maslow's_hierarchy_of_needs).
- "Mass Psychogenic Illness." *Wikipedia*, Wikimedia Foundation, 6 Apr. 2021, [https://en.wikipedia.org/wiki/Mass\\_psychogenic\\_illness](https://en.wikipedia.org/wiki/Mass_psychogenic_illness).
- "What Is Meaningness?" *Meaningness*, 8 May 2013, <https://meaningness.com/what-is-meaningness>.
- "A Gigantic Chart That Explains Absolutely Everything." *Meaningness*, 7 Sept. 2016, [meaningness.com/modes-chart](https://meaningness.com/modes-chart).
- "Metamodernism." *Wikipedia*, Wikimedia Foundation, 11 Apr. 2021, <https://en.wikipedia.org/wiki/Metamodernism>.

“Measures Governments Can Use to Promote Free Software - GNU Project - Free Software Foundation.” *A GNU Head*, <https://www.gnu.org/philosophy/government-free-software.en.html>.

Pinchevski, Amit, and Or Graur. “Memes in Digital Culture.” *The MIT Press*, The MIT Press, <https://mitpress.mit.edu/books/memes-digital-culture>.

Abd Kadir, Shamsiah, and Anitawati Mohd Lokman. “Persuasive Political Warfare.” [https://www.researchgate.net/publication/332471418\\_Memes\\_Persuasive\\_Political\\_Warfare](https://www.researchgate.net/publication/332471418_Memes_Persuasive_Political_Warfare).

“Memetic Engineering.” *Wikipedia*, Wikimedia Foundation, 8 Apr. 2021, [https://en.wikipedia.org/wiki/Memetic\\_engineering](https://en.wikipedia.org/wiki/Memetic_engineering).

Beritez-Bribiesca, Luis. “Memetics: a dangerous idea.” *Interciencia* 26.1 (2001): 29-31, <https://www.redalyc.org/pdf/339/33905206.pdf>.

Prosser, Michael B. *Memetics—A Growth Industry in US Military Operations*. MARINE CORPS UNIV QUANTICO VA SCHOOL OF ADVANCED WARFIGHTING (SAW), 2006, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a507172.pdf>.

“Memetics.” *Wikipedia*, Wikimedia Foundation, 30 Mar. 2021, <https://en.wikipedia.org/wiki/Memetics>.

“Memetic Warfare.” *Wikipedia*, Wikimedia Foundation, 5 Apr. 2021, [https://en.wikipedia.org/wiki/Memetic\\_warfare](https://en.wikipedia.org/wiki/Memetic_warfare).

Whip. “Micropayments Can Unlock ‘an Entire Economy’ between Ads and Subscriptions” *Digital Publishing News*, 6 May 2019, <https://whatsnewinpublishing.com/micropayments-can-unlock-an-entire-economy-between-ads-and-subscriptions/>.

“Microtransaction.” *Wikipedia*, Wikimedia Foundation, 25 Feb. 2021, <https://en.wikipedia.org/wiki/Microtransaction>.

Fields, R. Douglas. “Mind Reading and Mind Control Technologies Are Coming.” *Scientific American Blog Network*, Scientific American, 10 Mar. 2020, <https://blogs.scientificamerican.com/observations/mind-reading-and-mind-control-technologies-are-coming/>.

2021, Michael Cross 8 March. “Minister Hints at UK Departure from GDPR.” *Law Gazette*, 8 Mar. 2021, <https://www.lawgazette.co.uk/news/uk-to-depart-from-gdpr/5107685.article>.

Hancock, Brian J. “Memetic warfare: The future of war.” *Military Intelligence* PB 36.2 (2010): 41-46, [https://fas.org/irp/agency/army/mipb/2010\\_02.pdf](https://fas.org/irp/agency/army/mipb/2010_02.pdf).

Prange-Morgan, Chris. “Mitigating Absolutist Thinking.” *Psychology Today*, Sussex Publishers, 26 Mar. 2021, <https://www.psychologytoday.com/us/blog/full-catastrophe-parenting/202103/mitigating-absolutist-thinking>.

Government of Canada, Department of Justice. “Modernizing Canada’s Privacy Act.” *Government of Canada, Department of Justice, Electronic Communications*, 15 Feb. 2021, <https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html>.

“r/SlateStarCodex - Most of What You Read on the Internet Is Written by Insane People.” *Reddit*, [https://www.reddit.com/r/slatestarcodex/comments/9rvroo/most\\_of\\_what\\_you\\_read\\_on\\_the\\_internet\\_is\\_written/](https://www.reddit.com/r/slatestarcodex/comments/9rvroo/most_of_what_you_read_on_the_internet_is_written/).

Gundersen, Skrevet av Martin, et al. “My Phone Was Spying on Me, so I Tracked Down the Surveillants.” *NRKbeta*, <https://nrkbeta.no/2020/12/03/my-phone-was-spying-on-me-so-i-tracked-down-the-surveillants/>.

“Neoliberalism.” *Wikipedia*, Wikimedia Foundation, 14 Apr. 2021, <https://en.wikipedia.org/wiki/Neoliberalism>.

“Neuroscience-and the New Weapons of the Mind.” *Bulletin of the Atomic Scientists*, 26 July 2018, <https://thebulletin.org/2017/10/neuroscience-and-the-new-weapons-of-the-mind/>.

*New China Data Privacy Standard Looks More Far-Reaching than GDPR*, Center for Strategic and International Studies, <https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr>.

“New Human Rights to Protect against ‘Mind Hacking’ and Brain Data Theft Proposed.” *The Guardian*, Guardian News and Media, 26 Apr. 2017, <https://www.theguardian.com/science/2017/apr/26/new-human-rights-to-protect-against-mind-hacking-and-brain-data-theft-proposed>.

“Neuro-Marketing : Influencés Pour Consommer ?” *YouTube*, Universcience, 13 Aug. 2019, <https://www.youtube.com/watch?v=llwfcaY0S0>.

“New Media.” *Wikipedia*, Wikimedia Foundation, 11 Apr. 2021, [https://en.wikipedia.org/wiki/New\\_media](https://en.wikipedia.org/wiki/New_media).

George, Orwell. 1984. *Pandora’s Box*, 2017.

Mittal, Pardeep, and Jatinderpal Singh. “A Survey on Open Source Software using Questionnaire.” *International Journal of Computer Trends and Technology (IJCTT)* 4.4 (2013): 833-838.

Pandya, Jayshree. “Nuances Of Aadhaar: India’s Digital Identity, Identification System And ID.” *Forbes*, Forbes Magazine, 16 July 2019, <https://www.forbes.com/sites/cognitiveworld/2019/07/16/nuances-of-aadhaar-indias-digital-identity-identification-system-and-id/>.

“NZGOAL Software Extension.” *Data.govt.nz*, <https://www.ict.govt.nz/guidance-and-resources/open-government/new-zealand-government-open-access-and-licensing-nzgoal-framework/nzgoal-se/>.

Atwill, Nicole. *Online Privacy Law: France*, 1 June 2012, <https://www.loc.gov/law/help/online-privacy-law/2012/france.php>.

“On Mob Justice in the Tech Industry.” *Odysee*, <https://odysee.com/@Lunduke:e/MobJustice:6>.

Daigle, Leslie. “On the Nature of the Internet.” (2015), [https://www.cigionline.org/sites/default/files/gcig\\_paper\\_no7.pdf](https://www.cigionline.org/sites/default/files/gcig_paper_no7.pdf).

Zannettou, Savvas, et al. “On the origins of memes by means of fringe web communities.” *Proceedings of the Internet Measurement Conference* 2018. 2018, <https://dl.acm.org/doi/10.1145/3278532.3278550>.

“Open Access.” *Wikipedia*, Wikimedia Foundation, 3 Apr. 2021, [https://en.wikipedia.org/wiki/Open\\_access](https://en.wikipedia.org/wiki/Open_access).

“Open Source for Government.” *Open Source for Government*, <https://opensource.org/personas/government>.

Bakir, Vian, et al. “Organized persuasive communication: A new conceptual framework for research on public relations, propaganda and promotional culture.” *Critical Sociology* 45.3 (2019): 311-328, <https://journals.sagepub.com/doi/full/10.1177/0896920518764586>.

Rochat, Philippe. *Others in mind: Social origins of self-consciousness*. Cambridge University Press, 2009.

“Passion Economy Definition – What Is a Passion Economy?” *Mighty Networks*, 17 Mar. 2021, <https://www.mightynetworks.com/encyclopedia/passion-economy>.

Columbia Law Review. “PAYING FOR PRIVACY AND THE PERSONAL DATA ECONOMY.” *Columbia Law Review*, 27 Oct. 2017, <https://columbialawreview.org/content/paying-for-privacy-and-the-personal-data-economy/>.

“Percolation Theory.” *Wikipedia*, Wikimedia Foundation, 24 Jan. 2021, [https://en.wikipedia.org/wiki/Percolation\\_theory](https://en.wikipedia.org/wiki/Percolation_theory).

- “Personal Data Protection Bill, 2019.” *Wikipedia*, Wikimedia Foundation, 19 Feb. 2021, [https://en.wikipedia.org/wiki/Personal\\_Data\\_Protection\\_Bill,\\_2019](https://en.wikipedia.org/wiki/Personal_Data_Protection_Bill,_2019).
- “Persuasion.” *Psychology Today*, *Sussex Publishers*, <https://www.psychologytoday.com/us/basics/persuasion>.
- “Persuasive Technology.” *Wikipedia*, Wikimedia Foundation, 7 Apr. 2021, [https://en.wikipedia.org/wiki/Persuasive\\_technology](https://en.wikipedia.org/wiki/Persuasive_technology).
- McNamee, Roger. “Platforms Must Pay for Their Role in the Insurrection.” *Wired*, Conde Nast, <https://www.wired.com/story/opinion-platforms-must-pay-for-their-role-in-the-insurrection/>.
- Kuznetsov, I. S. “Political media memes’ persuasion and functioning in social media.” 22.2 (2017).
- Anderson, Tim. “Privacy Activist Max Schrems Claims Google Advertising ID on Android Is Unlawful, Files Complaint in France.” *The Register*, The Register, 7 Apr. 2021, [https://www.theregister.com/2021/04/07/max\\_schrems\\_google\\_complaint/](https://www.theregister.com/2021/04/07/max_schrems_google_complaint/).
- “View of Privacy as a Luxury Commodity: First Monday.” *View of Privacy as a Luxury Commodity*, <https://firstmonday.org/ojs/index.php/fm/article/view/3075/2581>.
- Holley, Peter. “Privacy as a Product: The Argument for Trading Your Personal Data to Get a Discount on a Car.” *The Washington Post*, WP Company, 17 Apr. 2019, <https://www.washingtonpost.com/news/innovations/wp/2018/06/26/privacy-as-a-product-the-argument-for-trading-your-personal-data-for-a-cheaper-car>.
- Walsh, Diana, James M. Parisi, and Katia Passerini. “Privacy as a right or as a commodity in the online world: the limits of regulatory reform and self-regulation.” *Electronic Commerce Research* 17.2 (2017): 185-203.
- “Product Placement.” *Wikipedia*, Wikimedia Foundation, 14 Apr. 2021, [https://en.wikipedia.org/wiki/Product\\_placement](https://en.wikipedia.org/wiki/Product_placement).
- bens6110. “What Is Promotional Culture?” *Promotional Culture - Critical Outlook*, 30 Nov. 2012, <https://promotionalcult.wordpress.com/2012/11/21/what-is-promotional-culture/>.
- Jowett, Garth S., and Victoria O’donnell. *Propaganda & persuasion*. Sage publications, 2018, [http://www.ffri.hr/~ibrdar/komunikacija/seminari/Propaganda%20&%20persuasion%20-%20difference%20\(Chapter1\).pdf](http://www.ffri.hr/~ibrdar/komunikacija/seminari/Propaganda%20&%20persuasion%20-%20difference%20(Chapter1).pdf).
- Cna. “Propaganda, Disinformation, & Other Influence Efforts: The Modern Information Environment.” *CNA*, <https://www.cna.org/centers/cna/cip/information-environment>.
- “Propaganda.” *Wikipedia*, Wikimedia Foundation, 17 Apr. 2021, <https://en.wikipedia.org/wiki/Propaganda>.
- Murphy, Elliot. “Psychic Life and the Power of Words.” *Psychology Today*, Sussex Publishers, 2 Apr. 2021, <https://www.psychologytoday.com/us/blog/language-and-its-place-in-nature/202104/psychic-life-and-the-power-words>.
- Clow, Ryan. “Psychological Operations: The need to understand the psychological plane of warfare.” (2008).
- “Psychological Warfare.” *Wikipedia*, Wikimedia Foundation, 12 Apr. 2021, [https://en.wikipedia.org/wiki/Psychological\\_warfare](https://en.wikipedia.org/wiki/Psychological_warfare).
- Anna, et al. “Racial Discrimination in Face Recognition Technology.” *Science in the News*, 26 Oct. 2020, <https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/>.

Staid, Mairead Small. "Reading in the Age of Constant Distraction." *The Paris Review*, 10 Dec. 2019, <https://www.theparisreview.org/blog/2019/02/08/reading-in-the-age-of-constant-distraction/>.

Zhang, Ruichen. "Re-directing socialist persuasion through affective reiteration: a discourse analysis of 'Socialist Memes' on the Chinese internet." *AI & SOCIETY* (2020): 1-12.

*Google Transparency Report*, Google, <https://transparencyreport.google.com/eu-privacy?hl=en>.

"Right to Internet Access." *Wikipedia*, Wikimedia Foundation, 15 Apr. 2021, [https://en.wikipedia.org/wiki/Right\\_to\\_Internet\\_access](https://en.wikipedia.org/wiki/Right_to_Internet_access).

*Right to Repair Europe*, 1 Mar. 2021, <https://repair.eu/>.

Gilbreath, Bob. "Rise of Subscriptions and the Fall of Advertising." *Medium*, The Graph, 24 Dec. 2020, <https://medium.com/the-graph/rise-of-subscriptions-and-the-fall-of-advertising-d5e4d880a49>.

Schwartz, Sarah. "Schools Teach 'Cyber Hygiene' to Combat Phishing, Identity Theft." *Education Week*, Education Week, 10 Dec. 2020, <https://www.edweek.org/technology/schools-teach-cyber-hygiene-to-combat-phishing-identity-theft/2018/03>.

"Screw It, I'll Host It Myself." *Marko Zivanovic*, 16 Apr. 2021, <https://www.markozivanovic.com/screw-it-ill-host-it-myself/>.

Scutti, Susan. "Self-Inflicted Injuries Surge among Tween and Early Teen Girls." *CNN*, Cable News Network, 21 Nov. 2017, <https://www.cnn.com/2017/11/21/health/self-inflicted-injury-cdc-study/index.html>.

"Self-Sovereign Identity." *Wikipedia*, Wikimedia Foundation, 2 Mar. 2021, [https://en.wikipedia.org/wiki/Self-sovereign\\_identity](https://en.wikipedia.org/wiki/Self-sovereign_identity).

Henson, H. Keith. "Sex, Drugs, and Cults. An evolutionary psychology perspective on why and how cult memes get a drug-like hold on people, and what might be done to mitigate the effects." *The Human Nature Review* 2 (2002): 343-355.

Perrin, Andrew, and Monica Anderson. "Share of U.S. Adults Using Social Media, Including Facebook, Is Mostly Unchanged since 2018." *Pew Research Center*, Pew Research Center, 7 Apr. 2021, <https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/>.

Jack Gillum, Justin Elliott. "Sheryl Sandberg and Top Facebook Execs Silenced an Enemy of Turkey to Prevent a Hit to the Company's Business." *ProPublica*, <https://www.propublica.org/article/sheryl-sandberg-and-top-facebook-execs-silenced-an-enemy-of-turkey-to-prevent-a-hit-to-their-business>.

"SIM, ESIM and Secure Elements." *Thales Group*, <https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/secure-elements>.

*Singer's Six Conditions - PAS Intervention*. [https://www.pas-intervention.org/uploads/2/2/5/4/22545256/singers\\_stages\\_of\\_mind\\_control.pdf](https://www.pas-intervention.org/uploads/2/2/5/4/22545256/singers_stages_of_mind_control.pdf).

"Slacktivism." *Wikipedia*, Wikimedia Foundation, 15 Apr. 2021, <https://en.wikipedia.org/wiki/Slacktivism>.

"Smart Doorbell." *Wikipedia*, Wikimedia Foundation, 24 Jan. 2021, [https://en.wikipedia.org/wiki/Smart\\_doorbell](https://en.wikipedia.org/wiki/Smart_doorbell).

*Snopes.com*, <https://www.snopes.com/>.

"Snowflake (Slang)." *Wikipedia*, Wikimedia Foundation, 6 Mar. 2021, [https://en.wikipedia.org/wiki/Snowflake\\_\(slang\)](https://en.wikipedia.org/wiki/Snowflake_(slang)).

- “Social Justice Warrior.” *Wikipedia*, Wikimedia Foundation, 28 Mar. 2021, [https://en.wikipedia.org/wiki/Social\\_justice\\_warrior](https://en.wikipedia.org/wiki/Social_justice_warrior).
- “Social Justice Warriors and Narcissism-What Is the Connection?” *Viva*, <https://vocal.media/viva/social-justice-warriors-and-narcissism-what-is-the-connection>.
- “Social Media and Social Problems: A Complex Link.” *RUSI*, 14 Nov. 2018, [https://rusi.org/commentary/Social\\_Media\\_and\\_Social\\_Problems\\_A\\_Complex\\_Link](https://rusi.org/commentary/Social_Media_and_Social_Problems_A_Complex_Link).
- “Social Media as a Public Utility.” *Wikipedia*, Wikimedia Foundation, 9 Feb. 2021, [https://en.wikipedia.org/wiki/Social\\_media\\_as\\_a\\_public\\_utility](https://en.wikipedia.org/wiki/Social_media_as_a_public_utility).  
(FSFE), Free Software Foundation Europe. *Public Money, Public Code*, <https://publiccode.eu/>.
- “Social Media Marketing.” *Wikipedia*, Wikimedia Foundation, 30 Mar. 2021, [https://en.wikipedia.org/wiki/Social\\_media\\_marketing](https://en.wikipedia.org/wiki/Social_media_marketing).
- Levy, Ro’ee. “Social media, news consumption, and polarization: Evidence from a field experiment.” *American economic review* 111.3 (2021): 831-70, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3653388](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3653388).
- “Spin (Propaganda).” *Wikipedia*, Wikimedia Foundation, 16 Apr. 2021, [https://en.wikipedia.org/wiki/Spin\\_\(propaganda\)](https://en.wikipedia.org/wiki/Spin_(propaganda)).
- Nyst, C., and N. Monaco. “How governments are deploying disinformation as part of broader digital harassment campaigns.” *Institute for the Future*, <https://www.iftf.org/statesponsoredtrolling/>.
- Waller, J. Michael. Strategic influence: *Public diplomacy, counterpropaganda, and political warfare*, [https://jmw.typepad.com/files/strategicinfluenceclass\\_copy.pdf](https://jmw.typepad.com/files/strategicinfluenceclass_copy.pdf).
- Whitepaper: Subscription Economy – Business Perspective*, <https://www.nets.eu/perspectives/Pages/Whitepaper-Subscription-economy-business-perspective.aspx>.
- Leslie, Alex. “Subscription Economy to Get a Real Boost from Advertising Fiasco.” *Disruptive Asia*, 21 Aug. 2019, <https://disruptive.asia/subscription-economy-boost-advertising-fiasco/>.
- Cass R. Sunstein, et al. *Sunstein on the Internet and Political Polarization*, University of Chicago Law School, <https://www.law.uchicago.edu/news/sunstein-internet-and-political-polarization>.
- “Surveillance Capitalism.” *Wikipedia*, Wikimedia Foundation, 15 Apr. 2021, [https://en.wikipedia.org/wiki/Surveillance\\_capitalism](https://en.wikipedia.org/wiki/Surveillance_capitalism).
- Barassi, By: Veronica. “Tech Companies Are Profiling Us From Before Birth.” *The MIT Press Reader*, 14 Jan. 2021, <https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/>.
- Lieber, Chavie. “Tech Companies Use ‘Persuasive Design’ to Get Us Hooked. Psychologists Say It’s Unethical.” *Vox*, Vox, 8 Aug. 2018, <https://www.vox.com/2018/8/8/17664580/persuasive-technology-psychology>.
- “Ted Chiang: Fears of Technology Are Fears of Capitalism.” *Kottke.org*, <https://kottke.org/21/04/ted-chiang-fears-of-technology-are-fears-of-capitalism>.
- Huntington, Heidi E. *Affect and effect of Internet memes: assessing perceptions and influence of online user-generated political discourse as media*, The. Diss. Colorado State University, 2017, <https://mountainscholar.org/handle/10217/183936>.
- THE BIG POTENTIAL OF BIG DATA*, Forbes Magazine, [https://www.forbes.com/forbesinsights/big\\_data/](https://www.forbes.com/forbesinsights/big_data/).

- Rushkoff, D., D. Pescovitz, and J. Dunagan. "The biology of disinformation: memes, media viruses, and cultural inoculation." *Institute for the Future* [= INSTITUTE FOR THE FUTURE «IFTF»] available at: [www.iftf.com](http://www.iftf.com).-Access mode: [http://www.iftf.org/fileadmin/user\\_upload/images/DigIntel/SR-2002\\_IFTF\\_Biology\\_of\\_disinformation\\_tk\\_042618.pdf](http://www.iftf.org/fileadmin/user_upload/images/DigIntel/SR-2002_IFTF_Biology_of_disinformation_tk_042618.pdf) (accessed 08.09. 2018) (2018).
- Cortez, Meghan Bogardus. "The Digital Citizenship Curriculum: Digital Literacy, Cyber Hygiene and More." *Technology Solutions That Drive Education*, 15 Sept. 2020, <https://edtechmagazine.com/k12/article/2018/04/digital-citizenship-curriculum-digital-literacy-cyber-hygiene-and-more-perfcon>.
- "The Digital Language Divide." *The Guardian*, Guardian News and Media, <http://labs.theguardian.com/digital-language-divide/>.
- Blog, Unsupervised. "The Dream of Neural Networks." *Medium*, Balabit Unsupervised, 10 July 2018, <https://medium.com/balabit-unsupervised/the-dream-of-neural-networks-6af1b6de704>.
- Taylor, Charles. *The ethics of authenticity*. Harvard University Press, 1992, <https://www.hup.harvard.edu/catalog.php?isbn=9780674987692>.
- Horrocks, Jarren. *The Future of Group Messaging*, <https://thejarren.com/group-messaging/>.
- Chercoles, Maria. "The Future of Your Privacy: Universal Right, Luxury, Commodity or Utility?" *Medium*, Matters, 1 July 2019, <https://medium.designit.com/the-future-of-your-privacy-universal-right-luxury-commodity-or-utility-a02b63f6afd6?gi=c45ef584c7a8>.
- AnonymousPlanet. *The Hitchhiker's Guide to Online Anonymity*, <https://anonymousplanet.org/guide.html>.
- Castells, Manuel. "The impact of the internet on society: a global perspective." *Change* 19 (2014): 127-148, <https://www.bbvaopenmind.com/en/articles/the-impact-of-the-internet-on-society-a-global-perspective/>.
- Busta, Caroline. "The Internet Didn't Kill Counterculture-You Just Won't Find It on Instagram." *Document Journal*, 16 Jan. 2021, <https://www.documentjournal.com/2021/01/the-internet-didnt-kill-counterculture-you-just-wont-find-it-on-instagram/>.
- "The Internet Way of Networking: Defining the Critical Properties of the Internet." *Internet Society*, 18 Dec. 2020, <https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/>.
- Stansberry, Kathleen, et al. "The Internet Will Continue to Make Life Better." *Pew Research Center: Internet, Science & Tech*, Pew Research Center, 9 July 2020, <https://www.pewresearch.org/internet/2019/10/28/4-the-internet-will-continue-to-make-life-better/>.
- Ng, Alfred, and Maddy Varner. "The Little-Known Data Broker Industry Is Spending Big Bucks Lobbying Congress." *The Little-Known Data Broker Industry Is Spending Big Bucks Lobbying Congress – The Markup*, <https://themarkup.org/privacy/2021/04/01/the-little-known-data-broker-industry-is-spending-big-bucks-lobbying-congress>.
- Blackmore, Susan, and Susan J. Blackmore. *The meme machine*. Vol. 25. Oxford Paperbacks, 2000, <https://www.susanblackmore.uk/the-meme-machine/>.
- "The Micropayment Economy: What It Is, and Why It Matters." *RSS*, <https://coinmarketcap.com/alexandria/article/the-micropayment-economy-what-it-is-and-why-it-matters>.
- Chekinov, Sergey G., and Sergey A. Bogdanov. "The nature and content of a new-generation war." *Military thought* 4 (2013): 12-23.
- Laufer, Daniel. "Russian Disinformation - The Network of Fake Foreign Media." *Netzpolitik.org*, 9 Dec. 2020, <https://netzpolitik.org/2020/russian-disinformation-the-network-of-fake-foreign-media/>.

- Moneyweek. "The Ongoing Rise of Big Tech." *MoneyWeek*, MoneyWeek, 21 July 2020, <https://moneyweek.com/investments/stockmarkets/601687/the-ongoing-rise-of-big-tech>.
- Firth, Joseph, et al. "The "online brain": how the Internet may be changing our cognition." *World Psychiatry* 18.2 (2019): 119-129.
- Scheff, Sue. "The People Behind Online Hate." *Psychology Today*, Sussex Publishers, 31 Mar. 2021, <https://www.psychologytoday.com/us/blog/shame-nation/202103/the-people-behind-online-trolling-shaming-cancel-culture>.
- Tyrrell, Mark. "The Dark Side of Your Emotional Needs – Connection." *Mark Tyrrell's Therapy Skills*, 4 Aug. 2019, <https://www.unk.com/blog/the-dark-side-of-your-emotional-needs-part-five/>.
- Tyrrell, Mark. "The Dark Side of Your Emotional Needs – Attention." *Mark Tyrrell's Therapy Skills*, 4 Aug. 2019, <https://www.unk.com/blog/the-dark-side-of-your-emotional-needs-part-one/>.
- Abbasi, Azad. "The Psychology Behind Social Media Lurkers." *Ignite Social Media Agency*, 19 Apr. 2016, <https://www.ignitesocialmedia.com/social-media-marketing/psychology-behind-social-media-lurkers/>.
- Haidt, Jonathan. *The righteous mind: Why good people are divided by politics and religion*. Vintage, 2012.
- Louis, Patrick. "The Self, Metaperceptions, and Self-Transformation." *Venam's Blog*, Patrick Louis Aka Venam, 24 Mar. 2020, <https://venam.nixers.net/blog/psychology/2020/03/25/self-perception-transformation.html>.
- "The Social Media Mindset." *Media Psychology Review*, 21 June 2008, <https://mprcenter.org/review/frenchsocialmediamindset/>.
- Young, Cathy, and 2015 June 18. "The Strange World of Social Justice Warriors." *Minding The Campus*, 29 June 2015, <https://www.mindingthecampus.org/2015/06/18/the-strange-world-of-social-justice-warriors/>.
- "The Booming Subscription Economy: A Win-Win for Brands and Affiliates." *TUNE*, 22 Feb. 2021, <https://www.tune.com/blog/subscription-economy-win-brands-affiliates/>.
- "The Subscription Economy: How to Focus Your Business Model on Subscribers, Not Just Products." *YourStory*, <https://yourstory.com/2018/12/subscription-economy-business-model/>.
- Freed, Richard. "The Tech Industry's Psychological War on Kids." *Medium*, Medium, 27 Apr. 2018, <https://medium.com/@richardnfreed/the-tech-industrys-psychological-war-on-kids-c452870464ce>.
- "The Trivium and "The Semiotic Iceberg": A Paradigm for Reading and Responding to Texts", <https://www.westga.edu/academics/coah/writing/assets/docs/uwc-handouts/semioticiceberg.pdf>.
- Madden, Jenae. "The 'We Live in a Society' Meme, Explained." *Happy Mag*, 16 Feb. 2021, <https://happymag.tv/we-live-in-a-society-meme-explained/>.
- The Whole Web Pays For Google And Facebook To Be Free*, Bloomberg, <https://www.bloomberg.com/opinion/articles/2021-03-03/pay-for-twitter-super-follows-you-can-thank-google-and-facebook>.
- "The World's Most Valuable Resource Is No Longer Oil, but Data." *The Economist*, The Economist Newspaper, <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

- “This Is What Happens When ICE Asks Google for Your User Information.” *Los Angeles Times*, Los Angeles Times, 24 Mar. 2021, <https://www.latimes.com/business/technology/story/2021-03-24/federal-agencies-subpoena-google-personal-information>.
- Crawford, Kate. “Time to regulate AI that interprets human emotions.” *Nature* 592.7853 (2021): 167.
- “Total War.” *Wikipedia*, Wikimedia Foundation, 11 Apr. 2021, [https://en.wikipedia.org/wiki/Total\\_war](https://en.wikipedia.org/wiki/Total_war).
- “REPORT Towards a More Sustainable Single Market for Business and Consumers.” *Europarl.europa.eu*, [https://www.europarl.europa.eu/doceo/document/A-9-2020-0209\\_EN.html](https://www.europarl.europa.eu/doceo/document/A-9-2020-0209_EN.html).
- Finkelstein, Robert. “Tutorial: Military memetics.” *Social Media for Defense Summit* 24 (2011).
- “Universal Integrated Circuit Card.” *Wikipedia*, Wikimedia Foundation, 20 Jan. 2021, [https://en.wikipedia.org/wiki/Universal\\_integrated\\_circuit\\_card](https://en.wikipedia.org/wiki/Universal_integrated_circuit_card).
- “Choosing Technology: an Introduction.” *GOV.UK*, <https://www.gov.uk/service-manual/making-software/open-source.html>.
- Nicki Lisa Cole, Ph.D. “What Does Weber’s Iron Cage Have to Do With Climate Change?” *ThoughtCo*, <https://www.thoughtco.com/understanding-max-webers-iron-cage-3026373>.
- Schiller, Ben. “Using Memes To Improve Climate Change Communication.” *Fast Company*, Fast Company, 8 May 2013, <https://www.fastcompany.com/1681526/using-memes-to-improve-climate-change-communication>.
- Chung, Andrew. “U.S. Supreme Court Rebuffs Facebook Appeal in User Tracking Lawsuit.” *Reuters*, Thomson Reuters, 22 Mar. 2021, <https://www.reuters.com/article/us-usa-court-facebook/u-s-supreme-court-rebuffs-facebook-appeal-in-user-tracking-lawsuit-idUSKBN2BE1TX>.
- Kopan, Tal. “US to Require Would-Be Immigrants to Turn over Social Media Handles.” *CNN*, Cable News Network, 29 Mar. 2018, <https://edition.cnn.com/2018/03/29/politics/immigrants-social-media-information/index.html>.
- “Virtue Signalling.” *Wikipedia*, Wikimedia Foundation, 16 Apr. 2021, [https://en.wikipedia.org/wiki/Virtue\\_signalling](https://en.wikipedia.org/wiki/Virtue_signalling).
- Dawkins, Richard. “Viruses of the mind.” *Dennett and his critics: Demystifying mind* 13 (1993): e27.
- Singer, Natasha. “‘Weaponized Ad Technology’: Facebook’s Moneymaker Gets a Critical Eye.” *The New York Times*, The New York Times, 16 Aug. 2018, <https://www.nytimes.com/2018/08/16/technology/facebook-microtargeting-advertising.html>.
- “Web Literacy.” *Mozilla Foundation*, <https://foundation.mozilla.org/en/initiatives/web-literacy/>.
- Giridharadas, Anand. “We Can Have Democracy or We Can Have Facebook, but We Can’t Have Both.” *The.Ink*, The.Ink, 10 Dec. 2020, <https://the.ink/p/we-can-have-democracy-or-we-can-have>.
- Toresson, Gustav Lundberg. “Welcome To The Passion Economy.” *Forbes*, Forbes Magazine, 18 Feb. 2021, <https://www.forbes.com/sites/gustavlundbergtoresson/2021/02/17/welcome-to-the-passion-economy/>.
- Austin, Drew. “Paid in Full.” *Real Life*, 19 Apr. 2021, <https://reallifemag.com/paid-in-full/>.
- Véliz, Carissa. “What Does Privacy Really Mean Under Surveillance Capitalism?” *Literary Hub*, 20 Sept. 2020, <https://lithub.com/what-does-privacy-really-mean-under-surveillance-capitalism/>.

- Cater, Leonie. "What Estonia's Digital ID Scheme Can Teach Europe." *POLITICO*, POLITICO, 13 Mar. 2021, <https://www.politico.eu/article/estonia-digital-id-scheme-europe/>.
- "What Is China's Social Credit System and What Does It Mean for Online Identity?" *SelfKey*, 25 Mar. 2020, <https://selfkey.org/chinas-social-credit-system/>.
- Williamson, Ann. "What is hypnosis and how might it work?." (2019): 1178224219826581, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6357291/>.
- What Is Propaganda, and How Does It Differ From Persuasion? *Propaganda and Persuasion* (Fourth Edition), <https://journals.sagepub.com/doi/full/10.1177/0896920518764586>.
- Messerly, John, et al. "What Is Social Cooling?" *Reason and Meaning*, 15 Jan. 2021, <https://reasonandmeaning.com/2017/10/31/what-is-social-cooling/>.
- Kumar, Rohan. "WhatsApp and the Domestication of Users." *Seirdy's Home*, 10 Mar. 2021, <https://seirdy.one/2021/01/27/whatsapp-and-the-domestication-of-users.html>.
- "What's Data Privacy Law In Your Country?" *Privacy Policies*, <https://www.privacypolicies.com/blog/privacy-law-by-country/>.
- "What's Going on With France's Online Hate Speech Law?" *Lawfare*, 24 June 2020, <https://www.lawfareblog.com/whats-going-frances-online-hate-speech-law>.
- Prijatel, Patricia. "Who Controls the Media? You'd Be Surprised." *Psychology Today*, Sussex Publishers, 8 Apr. 2021, <https://www.psychologytoday.com/us/blog/all-is-well/202104/who-controls-the-media-you-d-be-surprised>.
- "Who Runs the World... Big Tech?" *Global Witness*, <https://www.globalwitness.org/en/blog/who-runs-world-big-tech/>.
- Allyn, Bobby. "Why Is Facebook Launching An All-Out War On Apple's Upcoming iPhone Update?" *NPR*, NPR, 26 Feb. 2021, <https://www.npr.org/2021/02/26/971367875/why-is-facebook-launching-an-all-out-war-on-apples-upcoming-iphone-update?t=1614351654558>.
- Molloy, David. "Why Popular YouTubers Are Building Their Own Sites." *BBC News*, BBC, 6 Mar. 2021, <https://www.bbc.com/news/technology-55349255>.
- Elvy, Stacy-Ann. "Paying for privacy and the personal data economy." *Colum. L. Rev.* 117 (2017): 1369.
- "Woke." *Wikipedia*, Wikimedia Foundation, 14 Apr. 2021, <https://en.wikipedia.org/wiki/Woke>.
- Falkovich, Jacob. "The Narrative and Its Discontents." *Quillette*, Quillette Magazine, 17 Feb. 2021, <https://quillette.com/2021/02/16/the-narrative-and-its-discontents/>.
- "Above the Narrative." *Put A Number On It!*, 17 Mar. 2021, <https://putanumonit.com/2021/02/22/above-the-narrative/>.
- "Confirmation Bias in Action." *Put A Number On It!*, 6 Feb. 2021, <https://putanumonit.com/2021/01/23/confirmation-bias-in-action/>.
- "Shinkankakuha." *Wikipedia*, Wikimedia Foundation, 22 Nov. 2020, <https://en.wikipedia.org/wiki/Shinkankakuha>.
- Schreckinger, Ben, et al. "World War Meme." *POLITICO Magazine*, <https://www.politico.com/magazine/story/2017/03/memes-4chan-trump-supporters-trolls-internet-214856/>.
- Freddie deBoer. "You Can't Censor Away Extremism (or Any Other Problem)." *Freddie DeBoer*, Freddie DeBoer, 11 Mar. 2021, <https://freddiedeboer.substack.com/p/you-cant-censor-away-extremism-or>.

Ross, Pete. "Your Addiction to Outrage Is Ruining Your Life." *Medium*, The Bad Influence, 9 Aug. 2020, <https://medium.com/the-bad-influence/your-addiction-to-outrage-is-ruining-your-life-9effbdfeaca>.

*Zero Data App*, <https://0data.app/>.

Kumar, Manish, and Anwasha Mondal. "A study on Internet addiction and its relation to psychopathology and self-esteem among college students." *Industrial psychiatry journal* 27.1 (2018): 61.

"A Brief Introduction about New IP Research Initiative." *Huawei*, 13 Apr. 2020, <https://www.huawei.com/us/industry-insights/innovation/new-ip>.

"Discussion Paper: An Analysis of the 'New IP' Proposal to the ITU-T." *Internet Society*, 3 June 2020, <https://www.internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/>.

O'Donnell, Matthew Brook, Emily B. Falk, and Sara H. Konrath. "Big data in the new media environment." (2014).

Rilling, James K., and Alan G. Sanfey. "The neuroscience of social decision-making." *Annual review of psychology* 62 (2011): 23-48.

Rosling, Hans. "Anna Rosling (2018) Factfulness. Ten Reasons we're Wrong About the World-and Why Things Are Better Than You Think."

OVADYA, AVIV. "Contextualization Engines' Can Fight Misinformation without Censorship." *Medium*, Medium, 15 Apr. 2021, <https://aviv.medium.com/contextualization-engines-can-fight-misinformation-without-censorship-c5c47222a3b7>.

Halpern, Sue. "Facebook and the Normalization of Deviance." *The New Yorker*, <https://www.newyorker.com/news/daily-comment/facebook-and-the-normalization-of-deviance>.

Kegan, Robert, Lisa Laskow Lahey Robert Kegan, and Lisa Laskow Lahey. *Immunity to change: How to overcome it and unlock potential in yourself and your organization*. Harvard Business Press, 2009.

Kegan, Robert. *In over our heads: The mental demands of modern life*. Harvard University Press, 1994.

Rochat, Philippe. *Others in mind: Social origins of self-consciousness*. Cambridge University Press, 2009.

Serrano-Cinca, C., J. F. Muñoz-Soro, and I. Brusca. "A multivariate study of internet use and the digital divide." *Social Science Quarterly* 99.4 (2018): 1409-1425.

Stavropoulos, Vasileios, et al. "Flow on the Internet: a longitudinal study of Internet addiction symptoms during adolescence." *Behaviour & Information Technology* 37.2 (2018): 159-172.

Enagandula, Rupesh, et al. "Study of internet addiction in children with attention-deficit hyperactivity disorder and normal control." *Industrial psychiatry journal* 27.1 (2018): 110.

"Infographic: What Is Good Digital ID?" *McKinsey & Company*, McKinsey & Company, 13 Feb. 2020, <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/infographic-what-is-good-digital-id>.

Haidt, Jonathan. *The righteous mind: Why good people are divided by politics and religion*. Vintage, 2012.

Kahneman, Daniel. *Thinking, fast and slow*. Macmillan, 2011.

Brunton, Finn. "Constitutive interference: Spam and online communities." *Representations* 117.1 (2012): 30-58.

Floridi, Luciano. *The onlife manifesto: Being human in a hyperconnected era*. Springer Nature, 2015.

Metanomad. "The Battle Against the Hyperpresent." *Meta-Nomad*, 30 Nov. 2020, <https://www.meta-nomad.net/the-battle-against-the-hyperpresent/>.

The Economist. "Social media are turbocharging the export of America's political culture." *The Economist Newspaper*, Jun. 2021, <https://www.economist.com/international/2021/06/12/social-media-are-turbocharging-the-export-of-americas-political-culture>.

Paul Skallas. "Refinement Culture (PT 1)." *Refinement Culture (PT 1)*, Aug. 2021, <https://paulskallas.substack.com/p/refinement-culture>.

# Index

- 1 percent rule, 82
- 6th generation war, 61
  
- 1984, 98
  
- Aadhaar, 123
- AAR, 39, 70, 84
- absolutist thinking, 76, 89, 94, 103, 135
- abstract expressionism, 136
- activated ideology, *see* propaganda
- ad blocker, 110, 128
- agnotology, 16
- AIDA, 42
- algorithm amplification, 47, 63
- anonymity, 22, 56, 75, 108
- astroturfing, 63
- attention management, 128
- authenticity, 52, 87
- authority, 54, 137
- automatic detection systems, 126
- autonomous agents, *see* computational propaganda
- autonomy, 52
- awareness, 133
  
- Beck, 42
- Bernays, Edward, 136
- Big Brother, 99
- big data, 24
- biometric ID, 123
- Blackmore, Susan, 30
- bots, 63
  - social-bots, 63
- brain scan, 100
- Brave New World, 98
- bridge figures, *see* cognitive diversity85
- Brown, Wendy, 86
- buyer personas, *see* templatized83
  
- California Consumer Privacy Protection, 118
- Cambridge Analytica, 43
- cancel culture, 96, 99
- Capitalism Without Capital, 41
- CBT, 101
- censure, 13, 62, 99
- China 2035, 124
- China's Personal Security Specification, 120
- Cialdini, Robert, 16
- cognitive
  - attention, 55, 80
  - awareness, 99
  - memory, 55, 81
  - multi-tasking, 80
  - social cognition, 56, 81
- cognitive bias, 69, 133
  - attentional bias, 70
  - automation bias, 70
  - confirmation bias, 70
  - continued influence effect, 70
  - humor effect, 71
  - information bias, 71
  - picture superiority effect, 71
  - salience bias, 70
- cognitive dissonance, 16, 76
- cognitive diversity, 52, 74, 132, 136
- cognitive response, 70
- COIN, 65
- collectivists narrative, 95
- collusion, *see* conflicts of interests
- common goods, 91
- competency porn, 84
- computational propagandat, 22
- conflicts of interests, 106
- conspiracy theories, 93
- COPA, 117
- COPPA, 117
- corporatocracy, 87
- counterculture, 85
- cryptocurrencies, 112
- cult, 77, 86, 100
- cultural confusion, 16, 21, 32, 35, 52, 71, 73, 75, 87, 92, 134
- cyber hygiene, 123, 133
  
- Dada, 136
- data brokers, 45
- data collection, 25
- Data Protection Directive, 118
- Data Protection Officer, 119
- Davenport, 42
- Dawkins, Richard, 31
- declinism, 133
- deep dreams, 136
- deep fake, 15, 126
- DigiD, 123
- digital citizenship curriculum, 132
- digital divide, 85, 91, 109, 132
- digital identity, 120
- digital independence, 129
- discrimination, 84
- disinformation, 54, 93
- DNIE, 123
- dystopia, 98
  
- e-signature, 122
- economy
  - attention economy, 42, 99
  - data economy, 41
  - economic efficiency, 86
  - economic model
    - ad-supported, 107
    - freemium, 107

- micro-transaction, 110
  - PDE, 107
  - premium, 108, 132
  - privacy-discount, 108
  - subscription, 110
- fair competition, 106
- market solution, 105
- passion economy, 57, 110
- regulation, 105
- surveillance economy, 43
- EFF, 129, 133
- eIDAS, 121
- elaboration likelihood model, 33
- encryption, 127
- entrepreneurship, 53
- Erikson, Erik, 137
- escapism, 57, 134
- eSignature Directive, 122
- EULA, 48
  
- fact check, 133
- Factfulness, 133
- Falk, Emily, 74
- filter bubble, 74, 127
- Finkelstein, Robert, 36
- flag posts, 126
- free software, 129
- Freud, Sigmund, 136
- fringe ideas, 22, 27, 77, 83, 116
- FSF, 129
  
- Galloway, Scott, 109
- gatekeepers, 19, 94, 116, 127, 134
- GDPR, 118
- glocalization, 84, 114
- Golding, Sarah, 77
- GSMA Identity programme, 121
  
- Harris-Perry, Melissa, 96
- Hebrew University, 37
- hierarchies, 91
- Hilbert Martin, 51
- homophily, 74, 83
- Honest Ads Act, 118
- hormone, 70
- HSM, 122
- Huxley, Aldous, 98
- hyper-partisans, 64, 77, 83
- hypernormalization, 84
- hyperpresent, 99
- hypnosis, 101
  
- identity management, 121
- IFLA, 133
- Indiana University, 37
- individuation, 52, 74, 86, 90, 136
- influence, 11
- influencers, 134
  
- infobesity, 19, 81, 92
- information literacy, 131
- information management, 128
- infoxication, *see* infobesity
- intelligence gathering, 62
- interlocking monopolies, 106
  
- journalism, 93, 111, 116
  - citizen journalist, 54, 94
  
- Kegan, Robert, 137
- Kelly, Kevin, 42
- knowledge depth, 56
  
- language barrier, 51
- legal
  - accountability, 116
  - free speech, 48, 116
  - informed consent, 115
  - media regulation, 117
  - ownership, 115
  - privacy laws, 118
  - right of non-reception, 115
  - right to connect, 132
  - security, 116
  - transparency, 117
- Limor Shifman, 31
- Little, Arthur, 108
- lobbying, 48
- loneliness, 82, 92
- lurkers, 82
  
- marketing, 42, 86, 107
  - microtargeting, 43, 62, 77
- Maslow, Abraham, 137
- mass psychosis, 103
- mathwashing, 47, 84, 116, 127
- Maysles, Albert, 95
- McAdams, 52
- meaningness, 136
- media, 18, 54
- meme, 29
  - caricature, 54, 95
  - cognitive bias, *see* information bias
  - cult, 38
  - e-meme, 31
  - eunemics, 38, 89, 95
  - i-meme, 30
  - infotainment, 33
  - internet meme, 31
  - memeoid, 38, 77, 83
  - memeplexe, 33, 99
  - memetics, 30
  - memotype, 30
  - metamemetic thinking, 39, 134
  - military, 65
  - neoliberalism, 93
  - survival, 34

meta-data, 27  
 meta-modern, 135  
 micro-payment, 111, 127  
 mind-altering chemicals, 101  
 MOE, 61

national ID, 125  
 neoliberalization, 57, 86, 91, 114, 135  
 netizen, 51  
 normalcy, 83  
 nudge theory, 11, 22  
 NZGOAL, 130

open access, 129  
 open source, 129  
 open standards, 106, 120, 128  
 Organized Persuasive Communication, 12  
 Orwell, George, 98  
 outrage machine, 56, 96, 133  
 over-rationality, 135  
 Overton window, *see* fringe ideas, *see* fringe ideas

personal data, 24, 44, 100, 115  
     transitive propagation, 118  
 personified capital, 86  
 persuasion, 11  
 persuasive technology, 14, 46, 115  
     dark patterns, 46  
 Piaget, Jean, 137  
 polarization, 76  
 political discussion, 92  
 post-modern, 135  
 preconception, 75  
 privacy  
     privacy as a utility, 108  
     right, 114  
     sociality, 114  
 private justice, 56, 94, 134  
 privatization, 86  
 pro-social, 134  
 pro-social bots, 127  
 product placement, 11  
 promotional culture, *see* sub-propaganda, 77  
 propaganda, 12, 99  
     anchor, 15  
     black propaganda, 13, 117, 126  
     computational propaganda, 14, 63  
     counter-propaganda, 14  
     ethics, 17  
     grey propaganda, 14  
     hook, 15  
     imagery, 16, 64  
     meme, *see* meme  
     self-propaganda, 14  
     state, 59  
     sub-propaganda, 14  
     white propaganda, 13

psychic epidemic, 102  
 psychocivilized, 100  
 psychotronic weapon, 100  
 PSYOP, 60, 103

radicalization, 64  
 recommendation engines, 47, 94, 116, 117  
 relationships, 91  
 right to internet access, 84  
 Rossling, Hans, 133  
 Russia Federal Law on Personal Data, 120

satire, 95  
 schools, 132  
 sci-fi, 100  
 self-actualization, 137  
 self-authorship, 52  
 self-fulfillment, 85, 91  
 self-hosting, 128  
 self-inflicted injuries, 84  
 self-sovereign identity, 122  
 selfie generation, 52  
 semiotic, 33, 136  
 Shannon-Weaver communication, 10  
 shinkankakuha, 136  
 SIR, 34  
 SJW, 95  
 slacktivism, 21, 96  
 social alienation, *see* psychic epidemic  
 social bias, 71  
     authority bias, 72  
     grouptink, 72  
     reactance, 72  
     social comparison bias, 72  
     spotlight effect, 72  
 social confirmation, 74  
 social cooling, 57, 81, 121, 134  
 social media, 19  
     influencers, 57  
     politics, 21  
     profiles, 20, 25, 75  
     public utility, 22, 120  
 social media engagement, 20  
 social tribalism, 95  
 society  
     information society, 21, 51, 75  
     low-context society, 21  
 speech as a censorial weapon, 62  
 spin doctors, *see* propaganda  
 spinmeisters, *see* propaganda  
 Sunstein, Cass, 76  
 superusers, 82  
 surrealism, 136  
 symbolism, *see* semiotic

Taylor, Charles, 76  
 templatized, 83, 89, 99  
 third-party marketing, 25

total war, 60  
traceability, 122  
    supply chain, 124  
transparency, 128  
troll, 64  
true believers, see hyper-partisans77  
trust, 54, 75, 92, 105, 127  
    distrust, 89  
truth, 109  
  
UICC, 122  
University of Memphis, 36  
University of Pennsylvania, 74  
  
virtue signalling, 74, 96, 134  
VPN, 108, 128  
  
web literacy, 131  
  
Zeman, Zbyněk, 13  
zero-data applications, 128

End.