Implicit Trust and User Understanding

Team: Charlotte, DeLovell, Nikita

Intro & Background

In 2016 the world learned just how far-reaching the impact of implicit trust and user understanding could be, when Donald Trump was elected president in the United States, and Britain voted to exit the European Union. Subsequently, it came to light that a marketing company, Cambridge Analytica was largely responsible for skewing election results in both countries by using propaganda in the form of ads targeted towards groups of swing voters via social media to sway election results.

In a 2018 Senate Judiciary and Commerce Committee hearing, it came to light that these ad campaigns were hugely successful for two reasons, 1. Cambridge Analytica targeted customers by illicitly collecting their data in seemingly harmless online surveys through social media 2. They leveraged the privacy laws designed to protect consumers to keep the content of these ads and private, and covert. The impact of these ads even shocked Mark Zukerberg. In a 2018 Judiciary Committee hearing Zuckerberg said, "It's clear now that we didn't do enough to prevent these tools from being used for harm as well. That goes for fake news, foreign interference in elections, and hate speech, as well as developers and data privacy. We didn't take a broad enough view of our responsibility, and that was a big mistake."[1]

It has become a recurring theme that users are unaware of what data is being collected and how that data is being used. Companies publish their terms of service (TOS) as a means to protect themselves, but bury or obscure details as to how the data is being used in verbose legal jargon or "small print". Therefore, TOS are often overlooked by users, which puts users in a vulnerable position where they lack complete understanding and can be taken advantage of. Cambridge Analytica violation of data use is a ringing example of user ignorance, as it preyed on people using social media as a tool for social interaction and "fun," in this instance, using the survey as a get-to-know-me-better tool.

Even when more media literate users understand that their user trust may be violated, there is apathy and acceptance around the inevitability of user violations and the fact that there are often no alternatives. For example, most iPhone or Alexa users understand that their conversations are being recorded, but the

[1] Washington Post, "Democracy Dies in Darkness" April 9, 2018

problem is threefold--first, that there is no real way to turn off the recording devices in iPhones, google, or Alexa; second, these recordings enable the devices to operate “smarter” by gathering user information and feeding back targeted information to that user; third, competitor products all operate the same way, so there are no real alternative products available.

As a part of the Information Age, the advancement of technology and the world’s increasing use of technology is undergoing exponential growth. On our phones alone, new apps, widgets, and plugins are being created on a daily basis. The technology behind it is constantly evolving and being updated. Technology has always been designed to collect data as we go about our day-to-day. As companies discover that collecting, storing and selling user data is a more lucrative business model than simply selling the technology that collects, and uses the data this has become an escalating trend. Artifacts like location, app consumption, usage habits, purchases, conversations, and much more are being accumulated, sold, misused, and hacked as another source of revenue for a lot of the technology companies. Better practices by companies and more due diligence by users is spurred by the need to protect the user’s and bystander’s data as the world advances. The status quo is a liability to consumers and even third party bystanders as technology continues to advance and companies aren’t regulated in how Terms Of Service are presented.

Trends & Emerging Issues

It is evident that technology is changing at an alarming rate and in order to make a good case in predicting the future of Implicit Trust and User Understanding we started by collating signals. From that research, we had a better handle on the trends associated with our risk zone. We identified: growing amounts of data being collected and sold, negligent click-throughs of terms and conditions, ”smart” tech, facial recognition technologies, and awareness by organizations as evident and emerging trends.

What are the Signals?

SOCIAL. TECHNOLOGICAL. ENVIRONMENTAL. ECONOMIC. POLITICAL:

TREND: *Growing amounts of data being collected and sold at a premium.* Not only does this subject consumer data to undisclosed vendors who generally use such data for targeting ads, but it also leaves people more susceptible to security breaches as it exchanges hands of different entities

SIGNAL: Advertising (Economical)

One economical signal was uncovered in looking at the Interactive Advertising Bureau survey on user agreements. It reported that in 2018, $19 Billion was spent on consumer data just in the US. This price tag is an indicator of how data is being used to fuel targeted advertisements.

SIGNAL: Cambridge Analytica (Political)

Facebook's consumer data recently found its way into the hands of Cambridge Analytica who leveraged and sold data collected by the social media platform as a tool for political booster's who blasted misinformation to the targets in order to sway both the EU election as well as the 2016 United States Presidential election.

TREND: *Nondisclosure, low readability, misunderstanding of user agreements and no tech alternative leads to a rising number in "blind" click throughs.*

SIGNAL: Deloitte Survey (Economical)

A survey done by Deloitte provides a signal that is hard to ignore from an economical standpoint. The consulting firm found out that over 90% of consumers accept the terms and agreements without fully understanding them. A deeper breakdown of those surveyed found that the number increased to 97% when you look at the younger consumer demographic. This subset was made up of users in the 18-34 age range, which we could make inferences based on the demand for technology amongst the younger generations.

SIGNAL: Big Meat Comps (Environmental)

An environmental signal if this specific trend is the non-disclosure of information on the harm done to the environment by meat and dairy production companies based on their processes and byproducts which heavily contribute to greenhouse emissions as an environmental pollutant.

TREND: *“Smart” technology and aerial drones continue to trend upwards*, *catching the eye of many consumers and is finding its way into everyone’s daily lives.* The smartphones, smartwatches, smart speakers all have cameras and/or microphones embedded in them that, to the casual consumer, may seem innocent, but these advancements use the likes of AI to not only accumulate and sell but to learn and manipulate data that is being collected unbeknownst to the consumer.

SIGNAL: Alexa (Technological)

A look at two separate lawsuits involving Amazon’s Alexa provides another signal where technology perpetuates the risk of implicit trust and user understanding. The plaintiff, in both cases, claims that neither themselves (parents), nor the children agreed to have the child’s voice recorded, annotated, and stored by Amazon. The FTC has been brought into the case to conduct further investigations on the smart speaker.

SIGNAL: Ag Drones (Environmental)

Another environmental signal is displayed by the use of drones for agricultural tracking things like growth, livestock, resources, and geographical layout. While it helps farmers manage their local environment, it poses a privacy threat to oblivious neighbors and the farmers themselves as data is accumulated, stored, and redistributed.

TREND: *Across the world, facial recognition software being implemented into the likes of everyday cameras and surveillance.* Whether you agree to it or not, your face's data could be captured walking down the street, or as you accidentally photobomb a tourist in your city.

Across the world, facial recognition software is being implemented into the likes of everyday cameras and surveillance. Whether you agree to it or not, your face's data could be captured walking down the street, or as you accidentally photobomb a tourist in your city.

SIGNAL: T-Swift (Technological)

One instance is from 2018, where some of Taylor Swift's concert-goers found themselves subject to a kiosk that utilized facial recognition to cross-reference images with a list of "known stalkers" without the consent of the fans who indulged in the display.

SIGNAL: China Social Grading (Social)

Another signal comes from China where a Social Credit System that utilizes facial recognition technology in surveillance cameras across its major cities to identify the citizens, monitor their actions, and credits a score to them has been put into place. This score is piecemealed by local governments and various apps, and acts as a social marker and can lead to negative ramifications i.e. children not getting into good schools, getting your dog taken away, or being labeled a "bad citizen" effectively condemning one's social life.

While preceding trends and signals -- one diluting trend is awareness. While there is still minimal government regulation, organizations are being constructed to rate and monitor companies' terms and

conditions and are trying to do a better job in educating companies on creating ethical technology and features.

TREND: *While preceding trends and signals exacerbate the problem with Implicit trust and user understand-- one diluting trend is awareness.* While there is still minimal government regulation, organizations are being constructed to rate and monitor companies' terms and conditions and are trying to do a better job in educating companies on creating ethical technology and features.

SIGNAL: Government Regulations (Political)

Local US and EU governments have emerged to play a bigger role in setting and implementing regulations when it comes to data usage. As of right now, not a tone has been set as far as regulating implicit trust and user understanding, but this step (data) makes up a big part of what it a point of contention in the risk zone.

SIGNAL: Ethical OS (Social)

Ethical organizations, on the other hand, have started doing their parts in raising awareness in user agreements. Ethical OS, is one example. Other entities trying to change the social landscape that makes up the risk zone, as it is today, includes Coed Ethics and the Good Tech Conference. Perhaps awareness will constitute a resolution of the many risks that accompany implicit trust and user understanding.

Causal Layered Analysis

Causal Layered Analysis

Implicit Trust & User Understanding

LITANY

97% of Users Ages 18-34 accept T&A without fully understanding them.

It would take the average internet user 76 workdays to read all the terms of service they encounter.

Forrester predicts the global Big Data software market will be worth $31B this year.

There are 4.39 billion internet users in 2019.

Worldwide, 53% of online users are more concerned about their online privacy.

SYSTEMIC CAUSES

Big Data is delivering the most value by decreasing expenses and creating new avenues for innovation and disruption.

Companies who don't embrace BigData will lose market strength & may face extinction.

Data can be leveraged to influence elections.

User Agreements are there to protect the companies.

Little regulation to protect the end users or third parties beyond

WORLD VIEW

Lack of time.

Can't Trust the Government.

Anti- Corp- Libertarianism.

Individualism (users).

Capitalism --> anti-regulation

MYTHS & METAPHORS

You can't have your cake and eat it too.

A virus

Wolf in Sheep's Clothing

Rumplestiltskin

Highdsight is 20/20

Little Red Riding Hood

Big Tobacco

Using Sohail Inayatullah's Causal Layered Analysis (CLA) we looked at past and present contributing factors to the Implicit Trust and User Understanding risk zone. Comprised of four sections, we utilized the CLA as a means to paint a picture of all the elements Metaphors and Myths, Worldview, and Systemic Causes that led to the Litany on the subject today, which can be found in figure 1. In the appendix.

Litany

We started with Litany, which has been summed up as "the common but superficial understanding of the issue". Surface level risk zone constituted the following:

- companies invade privacy,
- Companies aren't transparent with they're use of consumer data,
- nobody reads the terms and conditions,
- the terms are hard to understand,
- there are no alternatives,
- companies deceive their users by selling data,
- misuse of data is a growing issue.

This was an exercise in empathy for some of us but also was an exercise in summarizing the main ideas that arose from conducting research. From there we were able to take another step back and ask what caused these thoughts on Implicit Trust and User Understanding.

Systemic Causes

We came up with a condensed list of systemic causes by looking at facts and data that came up in our research. Our list of causes consists of:

- societal apathy
- the price of data going up
- minimal regulation
- lack of tech alternatives when signing up
- covert business models
- technology advancement over policy
- low barriers to entry for new companies.

Worldview

Worldview, is understood by the group as humanity's past and evolved way of thinking on the subject in accordance with where we are now. The points we wanted to include in worldview are as follows:

- people want more tech capabilities (New! Now!)
- Trust is a big part of most cultures — most do not want to be taken advantage of.
- People enjoy their privacy.
- The United States sets the standard.
- Companies need to start taking ownership of their terms and services and accountability for the way data is used.

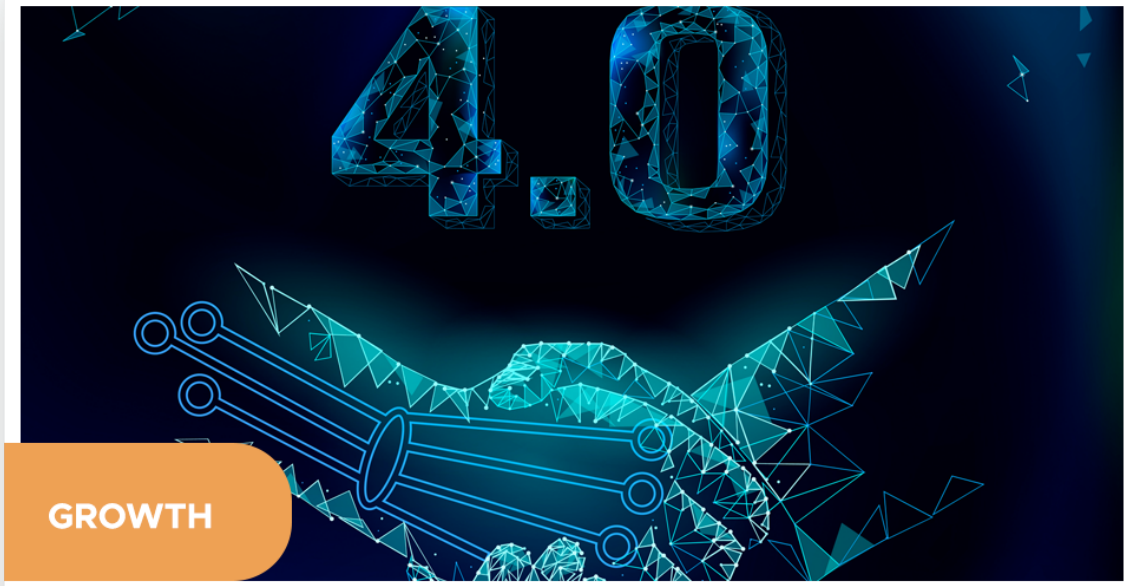
Metaphors and Myths

The final layer was probably the most fun. We came up with Little Red Riding Hood for her implicit agreement to come in the house and engage with the wolf with the thought that it was her Grandma, not realizing that Grandma was a wolf who planned to eat her. Big Tobacco did the same thing when they depicted cigarettes as fun, playful and cool, without being transparent about the dangers of smoking later down the road. Other examples we included in our CLA were "Ignorance is Bliss" which speaks to the younger generations' need for speed (tech advancement) and apathy for the terms and repercussions. , *Rumpelstiltskin* is a story of implicit adherence in which the King promises Rumpelstiltskin his first born grandchild in return for spinning straw into gold, not realizing the later consequences and negative ramifications of this promise later down the road. Finally, even Adam and Eve and the Forbidden Fruit highlights the implication of knowing you shouldn't do something but doing it anyway. I.e. user agreements and fine print.

Scenarios

In this section we will depict 12 futures scenarios around Implicit Agreement and User Understanding. Scenarios are set 20 years out, and have been deduced by taking into mind preceeding research and information. We will be utilizing three methodologies: Aleternate Futures, 2x2 Matrix, and Systems Mythology.

Alternative Futures

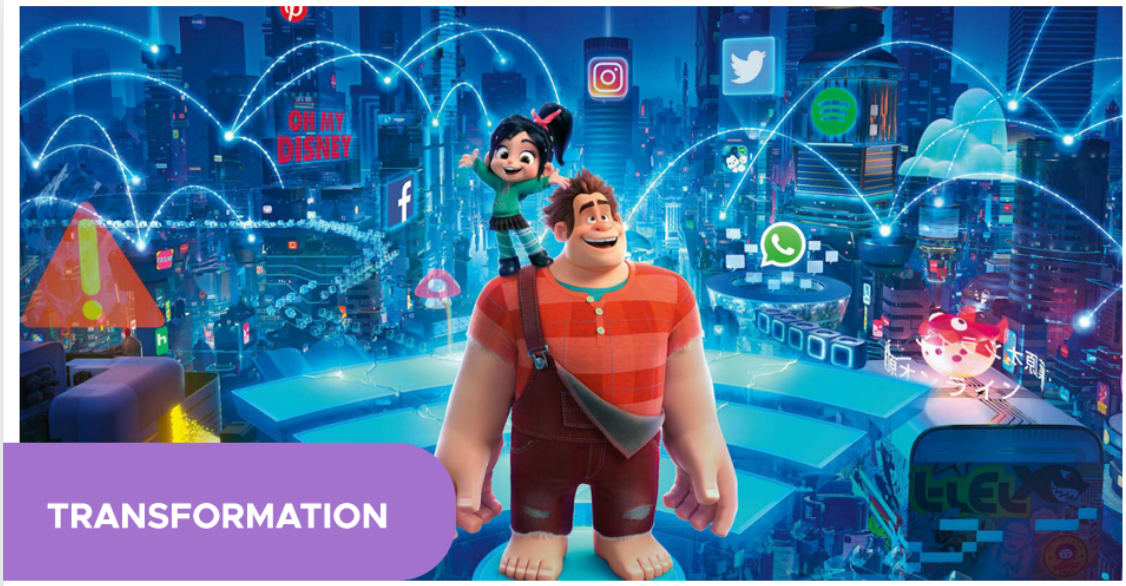


GROWTH

In this future, technology that looks scary today, is shaped by everyone's concerns, and gets better incrementally, and reaches a point where each year it feels more and more in line with societal expectations around privacy and control over data. Technology will become viewed as the trusted adult in the room, a source for absolute knowledge. Everyone settles into a new rhythm around how to interact better online, and companies like Facebook and Google adapt to user needs. Everyone trusts social networks more, and social networks get more trust-worthy. Securly incidents reduce, invasion of privacy reduces, fake news meet a match with tech that solves such issues, and overall the problem just diminishes in severity until it becomes a non-issue. The new reality that we settle into will then be the best of both worlds - tech driven benefits, but society driven control over privacy issues. The more we give technology, the better our own lives will become

DISCIPLINE

In this world, like growth we get better with tech and privacy, however this is achieved through heavy controls set up by regulations and certifications. Governments step in and create laws that companies need to adhere to. Consumers group together and create certifications. Companies that break laws are fined. Companies that don't certify and pass audits are avoided by consumers from buying considerations. Regulatory and competitive forces kick in, and the world moves to a model where everyone is forced to move to a discipline "overnight". Fact-checking will happen in all information in real-time to mitigate false and misleading claims. Technology will disregards everything from falsehoods to hyperbole so that facts cannot be skewed or misrepresented. Businesses complain, some businesses even die as their business model breaks, and there's generally a lot of angst, but the world then settles into a forced regimented discipline of following strict guidelines that consumers/society feels comfortable with.



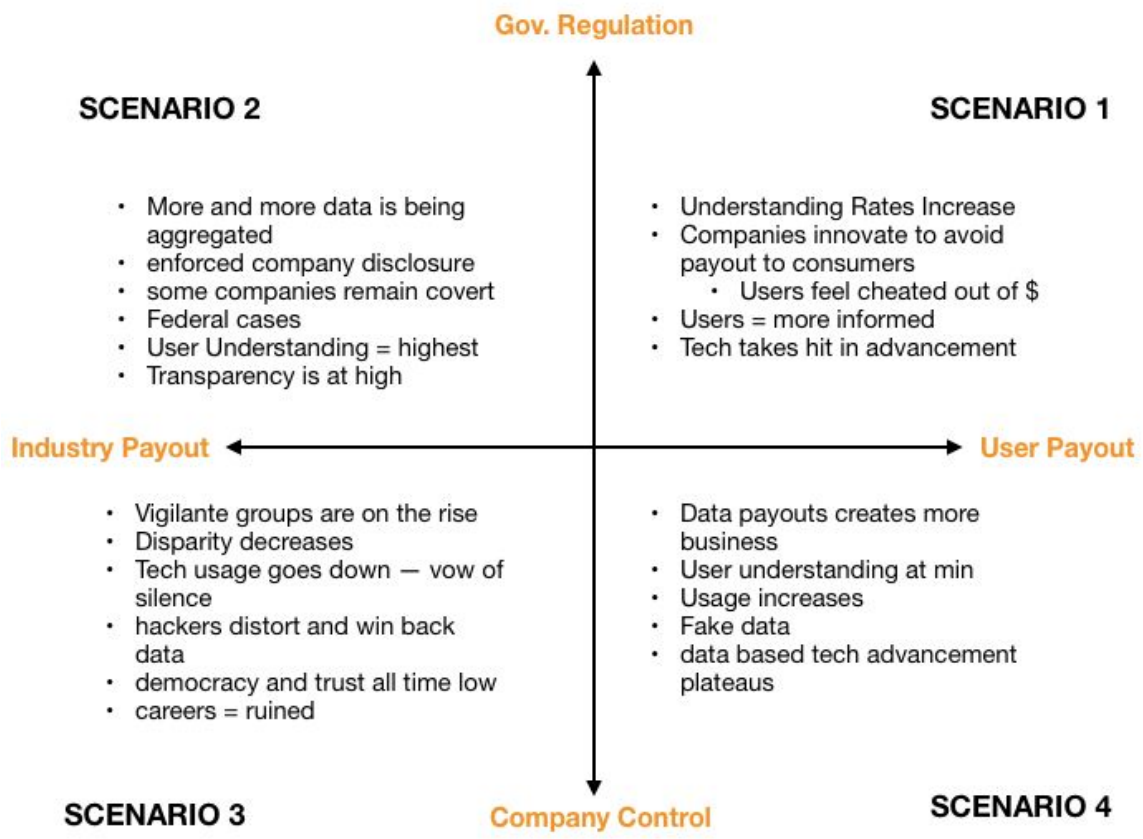
TRANSFORMATION

A new decentralized data layer is created where Facebook, Twitter, Google and YouTube like services become “open” - like Wikipedia, or like peer to peer file-sharing services. No one owns the data other than the original user, and it is always encrypted if it is ever transmitted or stored. Companies can’t sell your data, nor can users manipulate what you can or can’t see. Democracies aren’t threatened with political mud slinging on these networks, and the Internet basically becomes a very civil and self-regulating medium like the the real world we live in. The Internet looks dramatically different from where we are today - with perhaps a hit to online sales and e-commerce but with better outcomes for the society when it comes to safety, privacy, democracies, wars, etc. This reality is inspired by the vision portrayed in the show Silicon Valley and the above image is from Ralph, breaks the internet. Startup founders challenge the current world dominated by fake news, and lack of control of our data.

COLLAPSE

In this extreme future, there's complete erosion of trust in all information sources as news, editorials, and yellow journalism become more indistinguishable. Illiteracy rates rise as all printed words become viewed as a byproduct of corruption. The society watches helplessly as neither tech nor government is able to do anything to the issue of data privacy, fake news, and social media related anxiety. Countries get divisive, democracies are threatened, news is not reliable, people's deepest darkest secrets get leaked routinely, careers are destroyed, identity theft becomes rampant, insurance premiums become unbearable, citizens get unruly, social networking companies milk advertisement dollars from addicted consumers who can't get enough of their devices and online media, The mass adoption of a belief that the only truth is what one sees with their own eyes and everything else is false.

2x2 MATRIX



Scenario 1: AI Meet Data

Millions are tuned in on the Virtual™ as hundreds of protestors form outside of Facebook's data farming center, demanding they be paid for their data. Since the newly implemented taxation and compensation plan has been placed on companies, Big Tech has once again, turned to its AI partners to model data that used to be purely aggregated from its human-users. With human users being more educated on the product and the data that is being collected, companies are turning away from human data in order to avoid legal ramifications both in small claims and on the federal level. Today, humans are appealing, once again, to governing agencies to step in as they fee that this is just another move for the industry to separate themselves in an economic sense and are visibly frustrated as seen in their demonstration. Some are questioning the ability for tech to keep advancing with the migration away from collecting actual data from the users, but Mark Zuckerberg was quoted simply saying that they "have more than enough" human data to model after. While Facebook is the first, many others will follow — Big Tech gets exactly what they need at a much lower cost and allows them to incur less legal liability, something companies

are really trying to steer clear of after, what was, the largest class-action lawsuits of this era which nearly crippled the Trillion dollar business.

Scenario 2: We Rise: Trust, Transparency, and Technology

This year's Consumer Electronics Show (CES) might look a little different as regulation has skyrocketed especially in regards to user understanding and, once dreaded, Terms of Service agreement. Now that companies are now forced to disclose the data they are collecting, and state plainly, the use for it. This comes as a result of the governing agencies reaching a vote to increase the regulation as a way to advocate for users. So far this initiative has been good, and although there are still some users that are up in arms about not getting paid for their data, a recent Users of America poll showed that most users are content with getting a deeper look into the inner workings of the tech companies that continue to pump out the devices they love. The same poll also showed higher trust levels than ever before, which could also be indicated by the increased numbers of attendees at this year's show. As far as the companies that continue to be covert about their operations, the Federal Consumer Data Organization, and has been ruling with zero-tolerance and fights for transparency and envisions a day where products, services, and advertisements are becoming more and more efficient as a result of everyone being more open throughout the data usage timeline.

Scenario 3: We the Used

Following the worldwide public service announcement by the leader and "head hacker" of vigilante group "Forever Aware", people are filling the streets of Silicon Valley in what is drawing many parallels to the "Occupy Wallstreet" movement in the early twenty-teens. Surely proud parents watch on their V-sets as the movement looks to cast its shadow on the tech-filled valley — the call to action is based on the "head hacker's" recent statements that "something needs to be done" to stop the misleading actions of Big Tech. His group's recent attack on Big Tech sent waves across the world as his group infiltrated and stripped the data collection servers of Amazon Web Services; which Amazon is addressing to be what they believe was an inside job. Whether internal or external, the act to free the data was popular by demand. The threat looms to all in the Big Tech industry and arguments can be made that this will spark change as the possibility of losing users and data is ever-present.

Scenario 4: Fata Frenzy

Data Brokerage is one of the nation's trending businesses as data payouts have shifted to the users to create a 100 Billion dollar industry in just two years. User understanding and awareness are still at a minimum, but it doesn't seem to matter as the economical incentive has seemed to outweigh enlightenment and trust. While the GDP is on the rise, out as the additional income stream is being infused into all households helping millions climb above the poverty line, but Big Tech's biggest fear is a byproduct of the Fake Data. Fata Frenzy, one of the nation's top fake data players was breeched just last week amid the Valley's plea to government agencies, saying that the fake data is inhibiting their ability to continue to make technological advancements — "user greed" is to blame, and Big Data's attempts to enlighten the public on the data usage continue to be ignored as users keep their eyes on the award,

shifting their focus to the products and services that are offering the biggest payouts. Competition for authentic data is rising in the tech industry, and companies are seeing their bottom line increase as they try and fight for genuine users that are diminishing by the day amidst this modern-day gold rush.

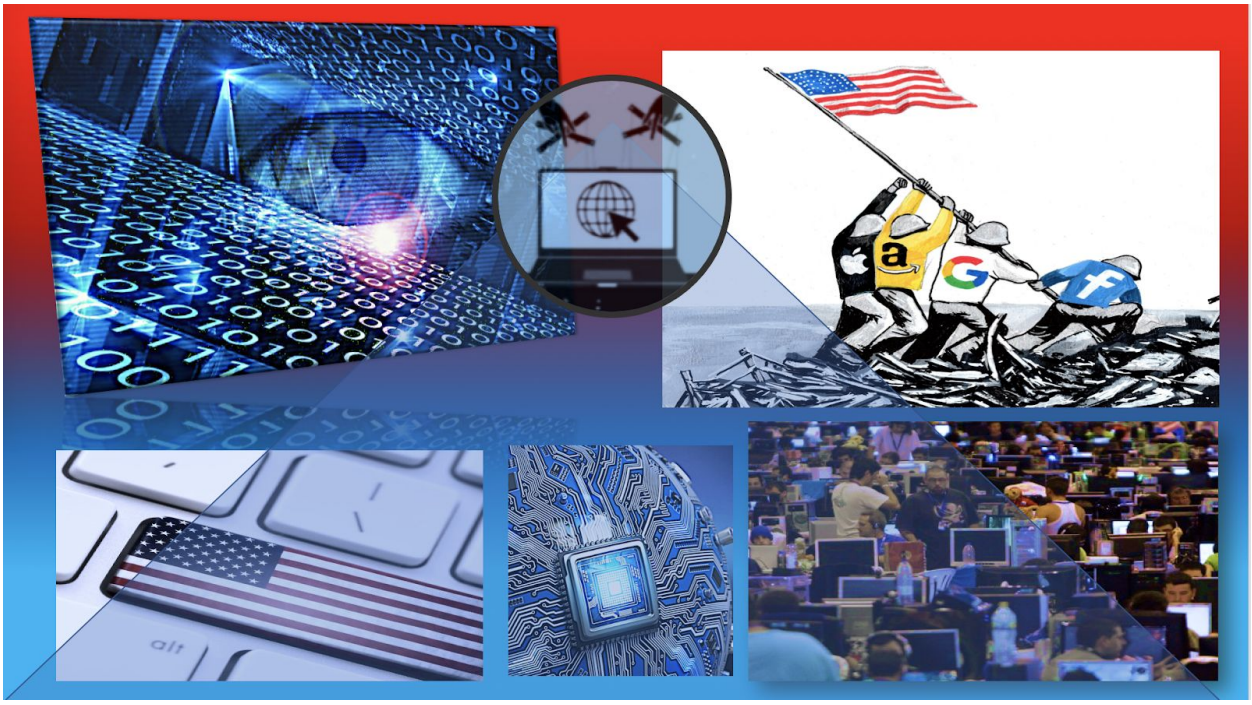
SYSTEMS MYTHOLOGY

Sovereign Identity—Blue & Purple

#ownyourdata becomes a movement. Each user has complete transparency over what data is being collected about them and how they are accessed. Individual identity which is fully controlled and maintained personally by the individual. Users own and control their personal data. Users may alter the set of permissions and revoke access to previously collected data at any given time. Blockchain is used to manage user privacy. Access-control policies are securely stored on a blockchain, where only the user is allowed to change them. Everyone has user encrypted digital identities. Self-monetizing personal data property rights becomes part of our commerce.

Cyberlibertarianism—Red & Purple

There is a backlash against government control over personal data and privacy. Vigilante groups resist government efforts to own, track and leverage user data pushing for free speech and absolutism. The country is in crisis. Data is the most valuable commodity but counter culture groups are fighting against mainstream, publicizing government interference and government intelligence. Technology is used by everyone as a way of life and it's accepted that big data is collected by the government which has grown more conservative and regulated. There is increasing political unrest. Technolibertarians embrace fluid, meritocratic hierarchies, oppose government over regulation and believe that the free market is the only rational choice.



Totalitarianism—Red & Blue

Government and big data companies have colluded for their own gain. The government has imposed conservative regulations over the economic and social structures so that while it mimics a free market, it is actually a non-market. Government is dangerously close to either a socialist or imperialist market economy. Big data companies are emboldened, displaying ostentatiously conspicuous patriotism to serve their own interests. To maintain order, the government has imposed regulations and curfew. Antitrust laws are in place. Data is convenience: Biometrics, facial recognition, and microchipping for tracking, employment, transit, commerce, and personal or private access is fully adopted and completely accepted. Through the use of technological advances, such as i5G connectivity and artificial intelligence, personal data is being used to determine viability for loans, insurance and credit. Citizens are tasked with tracking their own linkability-meta data in aggregate and reporting it to a central, government-controlled tracking system.

Eco Systems Solutions—Blue & Green

The government has imposed regulations on data privacy and rules are in place to ensure concise user agreements and a strong education movement around user privacy. #ownyourdata has made successful headway and data rights are viewed as human rights. However, there's been a major paradigm shift in our eco environment. Government have imposed regulations on living space, land-ownership, water and energy and food consumption. Architecture has been redesigned around modern day kibbutz community space, communal living, shared responsibility and ownership. Communal think tanks and hive minds are leveraging big data to find global energy, poverty, and agriculture solutions. Health care has been socialized, but there are firm restrictions around unnecessary procedures, with an emphasis on organic solutions such as nutritional, biotech, or rehabilitation. While some socialized solutions to health, food and energy are working brilliantly, the highly regulated way of life can be oppressive. Although data privacy is regulated, and citizens understand the importance of data ownership, the government use citizen data to control & regulate social systems related to land energy and food.