2nd David Farber Prize for Undergraduate Student Essay
First Prize
Edited 05. 2021

Lying in Wait
What Does More Data Mean for Us?

Leif Lincoln
Faculty of Economics
30 December 2020

A member of the *lepidoptera* order of insects — commonly known as butterfly — moves along close to the bio-diverse forest floor. Traversing from place to place it is looking for spots to stop, with flowers providing the ideal target. The mutually beneficial connection between the *lepidoptera* and flowers applies to those with the evolutionary advantage of flight. They come and go between the flowers which offer sweet nectar in return for pollination and the chance for reproduction. As the *lepidoptera* passes through the air bordering the forest floor, it spots the magnificent spectacle produced by a flower of the Orchidaceous order. This appears to be a perfect stop, for both rest and rejuvenation. But unbeknownst to itself, this orchid will ultimately become the *lepidoptera*'s final resting place.

The *Hymenopus coronatus*, also known as the walking flower mantis or orchid mantis, is a predatory insect native to the rainforests of Southeast Asia. With the brilliant colors of chartreuse, floral white, and violet illuminating its thorax and prothoracic shield, the mantis shows off eloquent beauty and an unmatched skill for imitation. As its name suggests, the mantis deceives its prey by imitating a blooming orchid, which is a source of food for many insects including *lepidoptera*. Contrary to common belief, the mantis does not hide in or among orchids. Instead, it exists disguised in plain sight and lies in wait for an unsuspecting visitor.

Life and industry in the 21st century are defined by the relentless progress and expansion of information technology with its unabating drive towards data collection. While computer processing power and hardware have also significantly advanced since the turn of the century, data is viewed as king. The value of information and data held on consumers is crucial to the business models of big tech companies. For these types of interactions between company and end user, the company provides a service. End user data constitutes the product to which advertisement, sales and other forms of monetizing manipulation are applied. This is the point then where society is inclined to jump the gun and scream "1984." As much as there are undeniable consequences and possibilities for the misuse of 'private' information at the industry or state level, there is also a profound misunderstanding of the underlying situation regarding data collection

and information technology. The most outstanding infringements of individual autonomy in information data seem to happen right in front of consumers' eyes, yet out of sight. If a tree falls in the forest and no one is around, does it make a sound?

Coexistence: Deception

Just as there is a connection between the butterfly, the flower, and the mantis in nature, a very similar, surreal situation exists in the realm of modern information technology. In this case, both consumers and technology companies support a mutually beneficial relationship. As a company provides a service to its consumer, the consumer helps the company repopulate its data store using two distinct methods: the human element and data provision.

The simpler of the two, the human element tends to act as a raw catalyst for consumer base growth through communication and social influences. Amidst influencers, social media, and even day to day online communication among social circles, the complex nature of interpersonal relations shows how the consumer base can expand through services on the information technology platform. This is equally true for products spread through traditional social contact. The social element has, time and time again, proved to be a decisive element for the sporadic but wide-reaching proliferation of certain products. Looking back at the "Tulip Mania" prevalent in Holland in the 1600's, word of mouth among consumers affected the breadth of the boom significantly. We see the working of the human element in the speculation that drove the tulip market to astounding heights. One *Semper Augustus* tulip bulb sold for astonishing prices in the tens of thousands of dollars in today's money (Garber, 1989). Evident in that market and in a multitude of similar situations throughout history, the human factor plays an undeniably significant role in the spreading and popularizing of products. Through trial and error, companies have come to understand the necessity of perfecting this capturing of the human element to maximize reach.

Data provision and its subsequent usage in the technology company, however, is a more complex topic. In this case, a company utilizes consumer data in order to reinvent and improve itself in an effort to grow. It does so by keeping tabs on search queries, personal information, and anything else that might find its way into its hands. Here consumer data is used to build efficiencies on the part of the company to provide a better platform with broader reach, just as the flower needs the butterfly to avoid stagnation and keep reproducing. The relationship between consumers and the company is an ever-evolving cycle beneficial to both parties as the consumer keeps consuming and the company growing.

The combination of these two seeding techniques puts the addition of new users (i.e., consumers) at the center, whereby the platform's growth is defined by the integration of human and data collection elements. This integration may be visualized in terms of a raceme, as found in flowers [Figure 1]. Each raceme, in turn, joins a larger panicle structure which represents the platform as a whole. Here the tree of connections illustrates the repetitive cycle of improvement, capture, and expansion of the platform.

Consumers and companies work hand in hand, providing mutual benefits for one another, but there is also the mantis. Not every flower is a mantis in disguise though the

threat of landing on one is very real. It is extremely difficult to determine the difference between a company with malicious or mischievous intentions from one with genuine intentions. The vast majority of data misuse happens behind closed doors out of the public eye. This is the case with phishing and other fraudulent activities hunting for data while mimicking the role of the mantis. These kinds of scams seek to profit by falsely representing widely trusted companies in both emails and websites. While these activities pose a significant security risk to consumers, they are often interpreted in pop culture and the media as a step toward an authoritarian dystopia based on false trust.

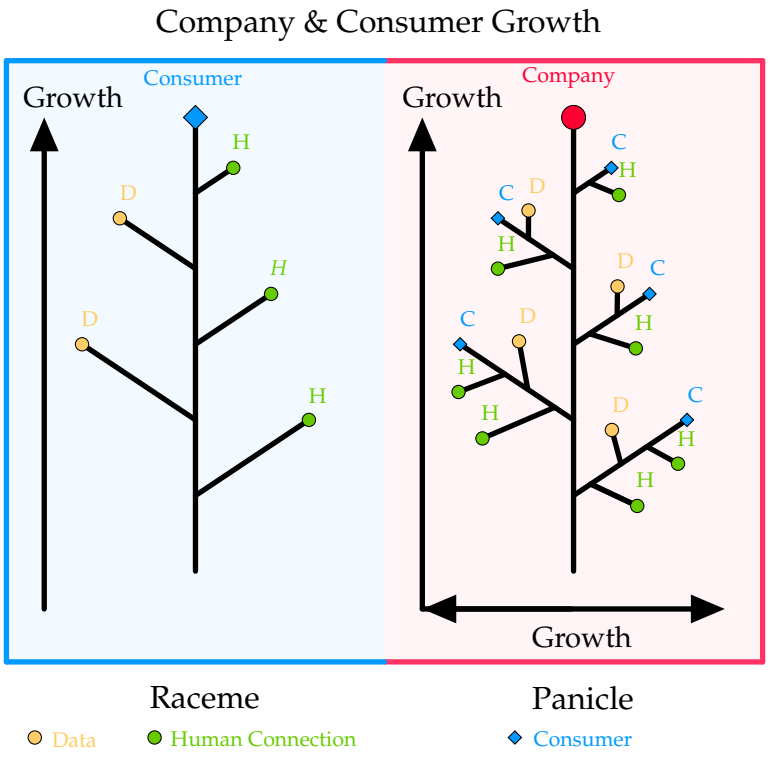

Figure 1: Visualizing the raceme and panicle structures.

On the other hand, the road to more concerning actions akin to authoritarian levels of power and control is a different type of 'pseudo-orchid' company that offers a real platform for consumers to benefit from while dishonestly using or collecting data. At first glance, this type of company would seem credible enough in providing a genuine service to their consumers; however, customer information and personal data would find their way into devious usage situations outside the platform's 'storefront.'

Most importantly, these companies maintain power over users through instilling trust in the unavoidability of their operations. Nathan Newman hints that if there is no realistic alternative for the services this type of company offers, consumers may not be able to stop providing information to it or see any way to cut themselves off from it (Newman, 2014).

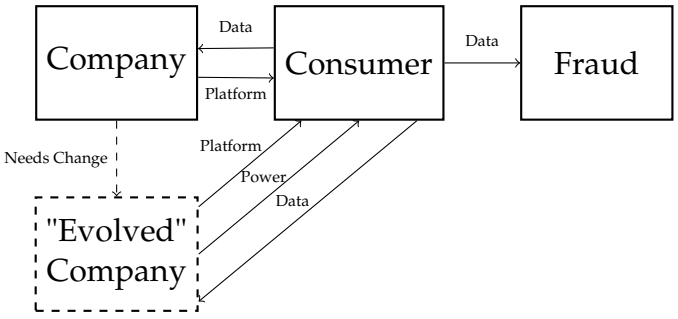

Figure 2: The tri-party ecosystem and the fourth party.

The real danger in this tri-party ecosystem of information technology is, in fact, not a distinct party at all. It is the mutant outgrowth of an environment that compels companies ballooning in size to surreptitiously take advantage of, prey on, and exploit their consumers. Unlike security breaches that characterize the actions of the mantis in the ecosystems, the rise of companies that exploit their consumers through credible trust is an entirely different breed [Figure 2]. This transformation is a prospect for any company or organization that manages the information of individuals. A trusted company today can become a 'trusted' predatory company tomorrow.

Dystopian Parallelisms

The notion of a dystopian era in which people succumb to a relentless government under the prudent eye of an oppressive overlord is a widely covered topic throughout history. From political rebels to thoughtful commentators, the fear of being pushed toward a situation of perceived despotism is a fear that, under given circumstances, all people seem to hold. How humans treat each other, historically, sheds light on this fear with the abhorring results of the battle for power: enslavement, persecution, and war. It is this fear that drives uncertainty with and opposition to the massive push of information technology and data collection that marks the 21st century.

To control one's fears, one must first understand them. The same is true regarding the prevention of a dystopian collision course. Power is vested in those with the propensity to exert change or authority over others. In the age of information technology, more data is more power. Even as companies and organizations collect an increasing amount of data from their consumer base, the bulk of data is not analyzed or used to effect and instead awaits its day in storage (Coughlin et al., 2017). It is from this storage that the greatest danger to privacy and individual autonomy come to light.

Collected data divides into two broad categories: active and passive data. Active data primarily encompasses the data which consumers give to companies. This information stems from the input fields when creating or updating an account, including sensitive data connecting users to the real world through bank accounts and addresses, though account numbers and names can hardly provide insight into the core thoughts and alignments of a person. Predictions, connections, and the very tuning of a person's mind all come from passive data inferences, i.e., the data the company collects without us even realizing it. Time elapsed, links clicked, and connected friends are all examples of the indicators that passive data goes out to capture (Younes, 2019). A given platform can record every action of the consumer to the smallest degree. This data and its usage are mostly unknown to the consumer as it works to build a digital image of their mind and preferences. This image is the link that connects the physical existence of a person to the map of his or her deepest corners of the mind.

Such a map can be viewed and analyzed in a large number of ways. For example, the data collected may provide (circumstantial) evidence of misguided action, serious blunders or breaking away from the wishes of the moderators in power, all of which could lead to self- condemnation if the person concerned only knew about it. A contemporary example of this behavior exists in the connection between pretextual evidence and unenforced law. Quite law-abiding citizens are at risk of breaking spurious, unknown

laws every day but go unpunished due to the mild nature of non-adherence. However, these unenforced laws act as the backbone for official pretext and a less than honest interaction with authorities (Blanks, 2016). Authorities might well enforce non-adherence with these laws not as a means of punishment for the underlying action but as one based on ulterior motives and thereby, in essence, bestow themselves power from the mere propensity to exercise it.

Driving in Los Angeles with an air freshener hanging from the rear-view mirror in violation of California Vehicle Code § 22708(a) — a minor law aimed at preventing obstruction of view which can be applied pretextually in such insignificant instants — will most likely not increase the likelihood of penalty subjection; yet, it is a testament to authorities' propensity to exert power. The same idea applies to technology companies. What do they do when they no longer need to focus on growing consumer numbers? The possibility for large, trusted companies to become predatory due to a stagnant or declining capturable population is nearing reality. Mega global tech companies no longer have the capturable population that they once did in their beginning years. A tight spot will cause companies to evolve and find new methods to maintain power and growth moving forward if they have not already begun to do so.

Big companies collecting big data pose a two-dimensional threat to individual autonomy and freedom if in the hands of a single governing entity possessing both the means and the motive to cross ethical boundaries. First, the immense stockpiling of personal information leaves individuals open to power abuse as everything is on record, no matter how insignificant. It is only human that people make mistakes, but information storage leads to the potential leveraging of that information. Second, the immense amount of data available to companies today leaves open the possibility of large-scale deception or manipulation through the fine-tuning of individual data consumption. Nathan Newman shows that large data companies have already begun to take advantage of the most vulnerable through behavioral profiling and the quoting of differential prices for goods and services (Newman, 2014). The dynamic fine-tuning of media preferences is cause for great concern given the abilities of and the extent to which those holding information on a person's preferences can go. Should companies or organizations that hold information resources fall under less than unanimous or outright malicious management, the autonomy of the individual will come under threat with potentially devastating effects.

Defining Privacy

Considering all the information the user provides freely, including that which is obtained through passive data, the question of privacy arises. Security is largely founded on the right to privacy. The tendency to entrust one's data and thereby one's safety over information platforms rests on the assumption that the data remains unknown to others. However, this trust also produces intense fear of both big data and the power that these keepers hold over the population on a personal level. Looking past the implicit security risk, it is essential to acknowledge how this potential guillotine over consumers' heads has changed the notion of privacy. What is it, and how has it changed since the dawn of the internet?

Before the advent of social media, the internet and even the dictaphone, accountability could not be purely objective. In primitive societies thousands of years ago claims of one individual against another did not — in themselves — provide a basis for the verification of truth. We can infer that although people were privileged to have complete privacy in this sense, they were no better off with it. Technology has given us the power to resolve such claims with verification. However, it is this very ability that people are now afraid of and which leads to calls for privacy protection. People are not inclined to trust technology that is not understood but rather trust the person in charge — for better or worse. At this point a problem arises in the modern age. How can consumers maintain privacy vis-à-vis controlling consumer data while also preserving the reliability and truthfulness that technology can provide? The answer lies in control. Consumers must return balance to the information ecosystem and oust manipulative, controlling, and dishonest practices while calling for autonomy over their own information. Current focuses on sensitive data protection do exist, such as demonstrated by the novel blockchain software. Still, the initiative to push for autonomous consumer control over all data collected both knowingly and unknowingly is not nearly strong enough. After all, it is the unknown that can hurt the most.

End Game — *Trust is Good, Control is Better*

The ability to afford trust is good, but control will always reign supreme. Tech companies and consumers alike both gain and lose substantially from changes in their ability to control information. Complete control over information allows companies and organizations to act in accordance with free will and bend the consumer to their desire. The next step, an oligopolistic consensus among information controlling authorities and management, would pose a grave risk to consumers with parallels to a 1984-like dystopian society, where authority has total control over its subjects. The simple tri-party system of two mutual beneficiaries and a clearly fraudulent predator to take advantage of this relationship is no longer dominant. A new party of malignant beneficiaries has arisen that is stronger than the swindling predator could have ever been, out to attract its prey, and exert and retain power. It is currently a minute to midnight where the future will come to rest in the hands of those with most control over information.

References

Blanks, J. (2016). Thin Blue Lies: How Pretextual Stops Undermine Police Legitimacy. *Case Western Reserve Law Review*, *66*(4), 931–946.

Coughlin, T., Hoyt, R., & Handy, J. (2017). https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/corporate/ieee-industry-advisory-board/digital-storage-memory-technology.pdf

Garber, P. M. (1989). Who Put The Mania In Tulipmania? *The Journal of Portfolio Management*, *16*(1), 53–60.

Newman, N. (2014). How Big Data Enables Economic Harm to Consumers, Especially to Low-income and Other Vulnerable Sectors of the Population. *Journal of Internet Law*, *18*(6), 11–23.

Younes, A. S. (2019). Passive Violation of Consumers' Privacy Rights on the Internet in the Age of Emerging Data Capital. *Journal of Content, Community and Communication*, *10*(9), 134–150.