

## Secrecy Unveiled: How Palantir Technologies Steals Your Right to A Secret

Sarah Kelly (She/Her)

University of British Columbia

### ABSTRACT

Secrecy and the maintenance of secrets have long been important sites of study for anthropology and other cognate disciplines, but few papers reflect on how the social power of secrets are supplanted when corporations are involved in taking secrets away from the individual. This paper reflects on the death of old notions of secrecy and the birth of modern notions of secrecy under a corporate capitalist system, and how previous anthropological thought on secrecy and power relations may be applicable to secrets. To do so, I examine how a data-mining company called Palantir displaces secrecy from the individual and their social sphere by constructing secrets as a piece of data to be bought and sold. Through examining previous anthropological thought and drawing on a case study of Palantir's operating system, Gotham; I intend to show that Palantir positions itself as a 'secret extractor' and how his reputation grants the corporation social power. However, this social power is not taken at no cost to social well-being; the extractive and unethical practices that Palantir uses to gather secrets are not being properly addressed.

### 1. Palantir and Secrets

Many corporations engage in some sort of secrecy, be that through patented knowledge unavailable to competitors or information that is obscured from the public eye, organizations regularly conceal information from the public, shareholders, and competitors (Federenko et al. 2023). While it is worth examining the implications of routine corporate secrecy, of particular interest to me are corporations that sell secrecy by extracting (often unwittingly to the subject) the secrets of others and construct themselves as "secret" corporate organizations. Palantir Technologies is a multi-billion dollar data-mining and analysis software company founded in 2004 using CIA seed money (Greenberg 2013; Johnson 2016).

Data-mining and analytics, at the broadest level, is a multistep process that involves taking large, often disparate, sets of data—this could be a structured database such as names and birthdates or streaming data like the live feed from a video—and integrating them on one platform and allowing users to interpret the data (Han et al. 2012). A major aspect of data analytics at Palantir is called link analysis, which involves looking for relationships between different entities in a data set (Types of Analysis). One of Palantir's flagship technologies, Gotham, relies heavily on link analysis to find people's names, car license plate information, or address. (Gotham). As of 2015, the last time a Palantir client list was leaked, Gotham was utilized by a large number of United States government departments, including the CIA, FBI, NSA, military, and municipal police departments (Burns 2015). Gotham, as an operating system, has broad applications and Palantir generally does not disclose how contractors may utilize the system (Gotham).

However, reporting has revealed that Gotham has been used to integrate previously siloed datasets between the FBI, to build a controversial license plate registry in California, and to create a vast and searchable network of data gathered from immigrants at the Mexico/United States Border (Burns 2015). In 2019, Palantir took over Project Maven from Google and is applying Gotham to AI drones used for bombing (Peterson 2019). The public rarely has access to information about the technologies that may be used to gather data about their lives, and fewer opportunities to decide if they want to allow this surveillance in their lives. It is important to consider how these corporate intrusions on the lives and secrets of individuals affect the person, their community, and our perception of such corporations.

Prior to examining how Palintir and its leadership uses secrets and the performance of secrecy as a tool for social domination, it is worth understanding what exactly secrets are- a challenge in and of itself. Secrets as an anthropological concept are particularly formidable to describe, as the obfuscation of knowledge exists in myriad forms to serve nearly endless sociocultural functions (Simmel 1906; Depenport 2019). “Knowledge” is of central concern to many anthropological research. I will extract a working definition of secrets from a historical understanding of knowledge studies in anthropology.

While there are many anthropological works that examine the impacts of contemporary surveillance on social relations, there are few articles that examine how Palintir’s extractive practices have repeatedly negatively impacted communal well being. Through understanding how secrecy and power have previously been considered, we can come to new conclusions about the influence of surveillance on our lives.

## 2. Social Importance of Secrets

Explicit engagement with limited fields of knowledge (logic, rationality, and cognition in particular) was one of the key disciplinary developments of anthropology in the 20th century (Boyer 2005). Contemporary anthropological research often aims to more adequately recognize and categorize so-called alternative forms of knowledge- indigenous knowledge and “local” knowledge (Hobart 1993). In these conversations, **non**knowledge has often been relegated to being the same as ignorance or a lack of knowledge. While studies of ignorance often debate the analytical or sociological interest of a lack of knowledge, they view nonknowledge as merely the negative inverse to the positive “true knowledge.” (Geisler 2013). This dichotomous understanding has the potential to prevent anthropologists from examining “not knowing” as a creative social form in its own right and a powerful discursive tool used in subjugation.

Within the field of not knowing, there is the more acute “secret”- whereas non-knowledge may be understood as the lack of something, secrecy contains an innate element of social performance. This distinction between not telling and telling is where philosopher Jacques Derrida argues that secrets exist- “here is a secret of denial [*dénégation*] and a denial [*dénégation*] of the secret. The secret *as such*, as secret, separates and already institutes a negativity; it is a negation that denies itself. It de-negates itself” (Budick & Iser 1996). By performing the telling or explaining of a secret or even by performing the not telling of a secret, the secret (knowledge) is simultaneously obfuscated yet reproduced. More powerful still at shaping the secret in a social and cultural setting is the performance of **obfuscation** of a secret. When one reports to another that something is “secret”, they simultaneously position themselves as a knower of secret knowledge (or at the very least, aware that such knowledge is secret) and the “secret” takes life as a social form. As Dave Boothroyd (2011) argues, “If no one knows it, it is not really a secret at all, and for this thing to be regarded as a secret in the first place, I must have already shared it with someone, or be able to share it—at the very least with myself” (47). The secret as a social form both grants knowledge of social life and affects the public perception of the secret holder.

From this, we can begin to understand that the social position of being known as a ‘secret holder’ will have some effect on the individual. Corporations, and their public-facing aspects, are also aware of this relationship. Palintir, and its co-founder Peter Theil, are intimately aware of the lurid appeal and social power that secrets have, he is quoted in an interview “very great business is built around a secret that’s hidden from the outside. A great company is a conspiracy to change the world; when you share your secret, the recipient becomes a fellow conspirator..” (Perell 2021). Yet, Palinitir does not adequately recognize or engage with the ethical and social implications of selling another person's secrets.

In conversations of secrecy and contemporary surveillance technologies, there is an unfortunate near-exclusive focus of the psychic harm caused by the blatant yet unavoidable surveillance of secrets that most people are subject to in their daily lives. Shoshana Zuboff's *The Age of Surveillance Capitalism* distills this attitude succinctly, "If we fail to take notice [of surveillance] now, how long before we are numb to this incursion and to all the incursions? How long until we notice nothing at all?" (2019, 327). What Zuboff and readers fail to grasp from this understanding is that having one's secrets observed does not merely create some higher-order, spiritual harm- rather these intrusions have devastating material effects on the lives of the observed. Through examining previous thought on secrecy, rather than 'not knowing', we can come to a clearer understanding of the power imbued in social relationships by secrecy.

Beyond an explicit political power, secrets are a deeply powerful social phenomena that exist in myriad ways across cultures. From Lurhman's (1989) work on secrecy in contemporary witchcraft practitioners in the United Kingdom in which she asserts that secrecy "creates value" and purveyors of secret knowledge have a way to safely enjoy a sense of control to Niko Besnier's (2009) ethnography on Nukulaelae atoll that explicated the social importance that gossip and secrecy has- secret gossip is simultaneously a tool that builds social bonds and reveals intricate social relations. Secrecy, as a discursive phenomenon, "can be used to characterize, categorize and organize virtually any kind of social fact" (Kirsh 2015, 102). In these ways, anthropologists can understand that secrets are far greater than the knowledge they conceal- secrets can be used to understand social power and relations.

If secrecy can be used to categorize and understand power, how does it affect the person when these secrets become points of data that can be bought rather than an interrogative and discursive tool that serve key social functions? What happens to the way we understand and relate to these corporations?

### **3. Gotham Sans Bat**

One of the companies most utilized products in Palantir Gotham, is surveillance technology. Palantir publicly markets these services as protecting American interests at home or abroad A featured quote on the Palantir website from General James N Mattis, former United States Secretary of Defence, of for Gotham states that "[Palantir] came up with groundbreaking technologies that help us make better decisions in combat zones. You are giving us advantages right now that we need." (Palintir). Palintir's business model is predicated on the extraction and selling of others' secrets. In fact, it is this reputation for being able to extract even the most closely held secrets that allows Palintir to have such a large market value and why their services are contracted to assist government agencies.

Palnitirs' ICM (Investigative Case Management) software, based on the Gotham platform, was used to facilitate ICE's (U.S. Immigration and Customs Enforcement) detention and deportation of the families of migrant children in 2017. ICM collects utilities data, housing data, DMV records, healthcare provider information, live cell phone recordings, and license plate images to build a profile on someone (Mijente 2017). This information is usually "secret" (ie, obfuscated from the general public) and typically requires a warrant to access if ICE is using traditional methods (Mijente 2018). However, when accessing this previously secret information through Palintir's technology, officers did require a warrant because this information was collected and aggregated by an outside contractor, rather than law enforcement.

According to an ICE (2017) handbook, ICE officers were instructed to use ICM to document any interaction they had with migrant children at the border. After a profile was created on the child and their family, Palintir's FALCON search engine,

also a part of the GOTHAM platform, was used to find links between ICM data sets to produce webs of relationships between individuals (Mijente 2017). This information was used to arrest and deport 433 individuals related to migrant children who themselves never came in contact with law enforcement (ICE 2017). It is essential to understand that these individuals would typically have not been deported, as those who are undocumented but do not come into contact with law enforcement are not. Individuals who requested to see reports on themselves or their children were denied, citing security concerns (ICE 2017). Immigration status *could* be viewed as a point of data, but this does not capture the “secret” that is one's illegal immigration status.

This view of immigration status as data not as “secret” does not capture that the public revelation of an undocumented immigration status and the consequences that follow is an extraordinarily destructive event to the lives and communities (Mckinnon 2018). Throughout the weaponization of ICM against migrants, Palintir's co-founder Alex Karp described Palintir's work with ICE as “very limited”, despite their contract with ICE in 2017 being the second-largest they had held (CNBC Television 2020). This is a purposeful obfuscation of the relationship that Palintir has with law enforcement. When it was revealed that Palintir's contributions were key to deportations, they faced no legal consequences or legislation limiting the use of their technologies.

To understand how this stealing of secrets creates power, we can use Michael Taussig's understanding of secrecy. Inspired by Elias Canetti's dictum, “secrecy lies at the very core of power” (1962, 90), Michael Taussig emphasizes the political importance of a secret. Taussig (1999) understands secrecy at the state level through the concept of a public secret, which he defines as “that which is generally known, but cannot be articulated.” These public secrets are indicative of hierarchical social orders, making domination unspoken. For Taussig, the ground of social power rests when one party is able to instruct another, “Even when X is generally known, you are enjoined to act and think as if X cannot be known.” It was known that Palintir was surveilling the public in this highly intrusive manner while simultaneously obfuscating this fact from the public, this is the definition of power.

It is the power to obfuscate knowledge, to be the one who dictates that which can be socially known and unknown that is most revealing of social power. Those who may have secrets are those in power, while those who are observed are subjugated (Taussig 1999). While Taussig found his site of understanding in fascist governments and other anthropologists have applied similar understandings of secrecy as the apoptosis of power to cults (see Pitt-Rivers 1997); this knowledge has rarely been applied to the modern, slick, corporate entities that functionally dominate contemporary North American society. Clearly, Palintir entrenched itself in the extraction of secrets and in doing so has positioned itself as a social entity of great power. In fact, it is this reputation that allows Palintir to be a highly profitable corporation.

By examining how Palintir, both the corporation and its employees, have the right to secrets but the subjects of their technologies do not, we can facilitate a new understanding of power relations that rests on the right to secrecy. Secrecy becomes an expression of power and commodity in its own right, those who have the privilege to remain opaque (such as tech billionaires) in an increasingly observed world are those who have power (Nuttal and Mbembe 2015).

We must aim to understand that these data-mining entities such as Palintir do not just extract non-socially charged pieces of data, they are taking secrets and creating a market value out of them. This is different from the state surveillance of the past, wherein secrets were extracted or created in pursuit of a larger political goal but did not have an explicit economic value (Manderson 2015). When it

becomes the right of a corporation to reveal secrets, this reinforces the existing power dynamics in which individual rights are subjugated under corporate interests. The dynamics of who can claim a secret and who exercises the right to tell that secret create new norms pertaining to the power of a secret, and are centrally linked to practices in today's capitalist society. If secrecy is central in creating and maintaining social relations of all forms, then we must understand how old notions of secrecy are displaced by "big data."

#### 4. The Price of Secrets

The monetization of secrecy is shaping a new power structure, one beyond previous understandings of secret knowledge and government interest. In this new age of secret extraction, corporations are not just acting to fill the needs of government surveillance, they are gathering secrets and billing themselves as knowers of secret knowledge for the express purpose of gathering social power which can be transformed into market value. When Palintir is viewed as a corporation that has the ability to gather lots of information, they undertake larger contracts and gain market value. However, these practices have not adequately been addressed in the legal sphere because this secret agething is existing beyond the government. Palintir's knowledge practices and personnel move across corporate-state boundaries and into the legal gray zones that emerge with the privatization of war and the outsourcing of intelligence functions (Welker et al. 2019).

I would be remiss to not mention that Palinitr agreed on January 14th, 2024 to assist the Israeli military in their ongoing genocide against the people of Gaza at the 2024 inaugural board meeting in Tel Aviv. (Newman 2024). Joe Lonsdail, a founding member of Palantir, said "Israel is now doing what it has to do to eliminate the bad guys...We are trying to make sure the U.S. stays more advanced to their enemies and keep them scared...So we were trying to keep the good guys armed and ahead" (Yadev 2023). This will likely involve integrating the data from Israeli surveillance technology with Palnitir's analytics tools, including Palantir Gotham. Palestinian people are unable to access the surveillance data that is produced about them, this knowledge becomes secret. (Abu Jabal 2020). This invasion into the private lives of Palistinians to gather data which will be used in a genocide against them is despicable. Israel has previously used unnamed algorithms on data gathered by the NSA. Hundreds of hours of phone calls between Palestinian Americans and their relatives in the West Bank were secretly exchanged to Israel in 2014, this information was used to arrest Palistians who committed no actual crime (Abrahms 2014). This unmitigated surveillance has never been addressed as unethical or illegal by Israel's international partners, and is allowed to continue. As the genocide continues, we must consdier the profit and power that corporate entities can access by being part of the killing machine.

It is of the utmost importance, beyond the academic exercise of exploring corporate secrets, that we recognize and understand who has the right to have secrets and thus, who has the right to live. As we enter a new age of surveillance and AI, corporations and their governing bodies must be forced to reckon with the fact that they are selling explicit social power- not mere points of data. Previous understandings of secrecy allow us to deeply understand how central and powerful secrets are to human livelihood, we must use his knowledge to hold corporations accountable and demand they cease opaque surveillance of us.

## References

- Asaro, P. M. 2013. The labor of surveillance and bureaucratized killing: New subjectivities of military drone operators. *Social Semiotics*, 23(2), 196–224. <https://doi.org/10.1080/10350330.2013.777591>
- Boothroyd, D. 2011. Off the Record: Levinas, Derrida and the Secret of Responsibility. *Theory, Culture & Society*, 28(7–8), 41–59. <https://doi.org/10.1177/0263276411423037>
- Boyer, D. (2005). Visiting knowledge in anthropology: An introduction. *Ethnos*, 70(2), 141–148. <https://doi.org/10.1080/00141840500141097>
- Gotham | Palantir.” n.d. [www.palantir.com](https://www.palantir.com). <https://www.palantir.com/platforms/gotham/>.
- Fedorenko, I., Berthon, P., & Edelman, L. 2023. Top secret: Integrating 20 years of research on secrecy. *Technovation*, 123, 102691. <https://doi.org/10.1016/j.technovation.2023.102691>
- [Han, Jiawei, Micheline Kamber, and Jian Pei. \*Data Mining: Concepts and Techniques, Third Edition\*. 3rd ed. Waltham, Mass.: Morgan Kaufmann Publishers, 2012.](https://doi.org/10.1016/j.technovation.2023.102691)
- Hannah, D., Parent, M., Pitt, L., & Berthon, P. 2014. It’s a secret: Marketing value and the denial of availability. *Business Horizons*, 57(1), 49–59. <https://doi.org/10.1016/j.bushor.2013.09.001>
- Herd, G. 1990. Secret Societies and Secret Collectives. *Oceania*, 60(4), 360–381.
- Hobart, M. 1995. An Anthropological Critique of Development: The Growth of Ignorance. *The Journal of the Royal Anthropological Institute*, 1. <https://doi.org/10.2307/3034254>
- Johnson, D. V. 2016. Improv-da: How Palantir has made corporate orthodoxy out of experimental theater. *The Baffler*, 32, 20–25.
- Luhrmann, T.M. 1989. The magic of secrecy. *Ethos* 17: 131–16
- Kirsch, T. 2015. *Kirsch\_ "Secrecy and the Epistemophilic Other" (2015)* (pp. 188–208).
- McKinnon, F. 2020. After Deportation: Ethnographic Perspectives. By Shahram Khosravi. *Migration Studies*, 8(3), 482–483. <https://doi.org/10.1093/migration/mny021>
- Mills, A. J. 2015. Everyone loves a secret: Why consumers value marketing secrets. *Business Horizons*, 58(6), 643–649. <https://doi.org/10.1016/j.bushor.2015.07.001>
- National Security Archive. n.d. “Palantir, the Palantir Platform: The Platform for Information Analysis, No Date. Not Classified. | National Security Archive.” [Nsarchive.gwu.edu](https://nsarchive.gwu.edu). Accessed May 13, 2024. <https://nsarchive.gwu.edu/document/15330-palantir-palantir-platform-platform>.
- Newman, M. 2024. Thiel’s Palantir, Israel Agree Strategic Partnership for Battle Tech. [Bloomberg.com](https://www.bloomberg.com/news/articles/2024-01-12/palantir-israel-agree-to-strategic-partnership-for-battle-tech?leadSource=uverify). <https://www.bloomberg.com/news/articles/2024-01-12/palantir-israel-agree-to-strategic-partnership-for-battle-tech?leadSource=uverify>
- Nuttall, S., & Mbembe, A. 2015. Secrecy’s Softwares. *Current Anthropology*, 56(S12), S317–S324. <https://doi.org/10.1086/683295>
- “Types of Analysis.” n.d. Palantir. Accessed May 11, 2024. <https://www.palantir.com/docs/foundry/analytics/types-of-analysis/>.
- Palantir. (n.d.). *Palantir Privacy and Security Statement*. Palantir. Accessed January 29, 2024, from <https://www.palantir.com/privacy-and-security/>

- Pompliano, P. 2020. *Why Peter Thiel Searches for Reality-Bending “Secrets.”*  
<https://www.readtheprofile.com/p/peter-thiel-secrets>
- Scott, C. R. (2013). “Unmasking What We Know about Hidden Organizations.” In C. Scott (Ed.), *Anonymous Agencies, Backstreet Businesses, and Covert Collectives: Rethinking Organizations in the 21st Century* (p. 0). Stanford University Press.  
<https://doi.org/10.11126/stanford/9780804781381.003.0002>
- Security: A Conversation with the Authors | Cultural Anthropology*. n.d.. Retrieved January 28, 2024, from  
<https://journal.culanth.org/index.php/ca/security-conversation-with-the-author>  
s
- Yadav, N. 2023. “Palantir Co-Founder Discusses Company’s Role In Helping Israel Amid War With Hamas, Stresses Need To Keep “Good Guys Armed And Ahead” - Palantir Technologies (NYSE:PLTR). *Benzinga*.  
<https://www.benzinga.com/news/23/11/35560418/palantir-co-founder-discusses-companys-role-in-helping-israel-amid-war-with-hamas-stresses-need-to-k>