UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Mapping Interfacial Regimes of Control: Palantir's ICM in America's Post-9/11 Security Technology Infrastructures

Knight, E.; Gekker, A.

DOI
10.24908/ss.v18i2.13268

Publication date
2020

Document Version
Final published version

Published in
Surveillance & Society

License
CC BY-NC-ND

Link to publication

Citation for published version (APA):
Knight, E., & Gekker, A. (2020). Mapping Interfacial Regimes of Control: Palantir's ICM in America's Post-9/11 Security Technology Infrastructures. *Surveillance & Society*, *18*(2), 231-243. https://doi.org/10.24908/ss.v18i2.13268

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:16 Sep 2026

Surveillance & Society

Article

Mapping Interfacial Regimes of Control: Palantir's ICM in America's Post-9/11 Security Technology Infrastructures

Emma Knight

University of Amsterdam, The Netherlands
emmakknight@gmail.com

Alex Gekker

University of Amsterdam, The Netherlands
a.gekker@uva.nl

Abstract

Recent technological advancements in surveillance and data analysis software have drastically transformed how the United States manages its immigration and national security systems. In particular, an increased emphasis on information sharing and predictive threat modeling following the terrorist attacks of September 11, 2001, has prompted agencies such as the Department of Homeland Security to acquire powerful data analysis software from private sector vendors, including those in Silicon Valley. However, the impacts of these private sector technologies, especially in the context of privacy rights and civil liberties, are not yet fully understood. This article interrogates those potential impacts, particularly on the lives of immigrants, by analyzing the relational database system Investigative Case Management (ICM), which is used extensively by Immigration and Customs Enforcement (ICE) to track, manage, and enforce federal immigration policy. As a theoretical framework, we use Benjamin Bratton's concept of the "interfacial regime," or the layered assemblages of interfaces that exist in modern networked ICT infrastructures. By conducting a document analysis, we attempt to visually situate ICM within the federal government's larger interfacial regime that is composed by various intertwined databases both within and outside the government's realm of management. Furthermore, we question and critique the role ICM plays in surveilling and governing the lives of immigrants and citizens alike.

Interfacialization of Control in Post-9/11 US Border Security

Recent technological advancements in surveillance and data analysis software have drastically transformed how the United States manages its immigration and national security systems. In the "post-Snowden" era (Lyon 2015), the broader concern over the imbrication of technological ubiquity with surveillance has particular urgency when examining borders that existed as extrajudicial space even before the advent of digitalization (Johnson 2014). Certainly, the adoption of "smart" technologies in border security has increased the federal government's ability to identify and prevent terrorist attacks and other threats to the nation's security. However, the unquestioned embrace of such technology has prompted many to consider the implications of its use, especially in the context of the United States' current political climate surrounding immigration. As Louise Amoore and Rita Raley (2017: 4) succinctly ask, "What are the political and ethical stakes involved in securing with, through, and via algorithms in the 21st century?"

Further moral and political questions arise when one examines the private sector companies that build and sell the algorithms, software products, and databases that the American immigration system now relies upon. Silicon Valley companies have secured substantial contracts with the federal government and are largely responsible for the current technology architectures at agencies such as the Department of Homeland Security (DHS) (Mattern 2018). One company in particular, Palantir Technologies, provides the DHS with software called Investigative Case Management (ICM), which has been described as the "core law

Knight, Emma, and Alex Gekker. 2020. Mapping Interfacial Regimes of Control: Palantir's ICM in America's Post-9/11 Security Technology Infrastructures. *Surveillance & Society* 18(2): 231-243.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487
© The author(s), 2020 | Licensed to the Surveillance Studies Network under a Creative Commons Attribution Non-Commercial No Derivatives license

enforcement tool" used by the DHS's sub-agencies Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), and Enforcement and Removal Operations (ERO) (Woodman 2017).

ICM gathers personally identifiable information by interfacing with a variety of other databases; these include not only those within DHS, but also those housed in other federal, state, and local agencies, as well as with commercial databases (Mijente, The National Immigration Project, and Immigrant Defense Project 2018). As an interfacial software application itself, ICM thus exists within a larger "interfacial regime," a concept articulated by Benjamin Bratton (2015: 229) that captures the philosophical dimensions of the ways in which interfaces "organize the actions of Users." In this manner, interfacial regimes can be understood as an assemblage of interfaces, such as ICM's interconnected database network, which can consequently exert considerable governing influence over the actions of users.

We see this concept as a useful addition to the toolkit of surveillance studies scholars in their expanding work on the imbrication of technologies, tracking, and control. So far, the majority of this scholarship has been focused on *dataveillance* (Clarke 1988; Amoore and De Goede 2005; Van Dijck 2014), or the implications of mass personal data collection by governmental and corporate actors for the freedom of citizens and users. In particular, this has led to several recent attempts to define the scholarly boundaries of the phenomenon, termed, among others, datafication (Van Dijck 2014), surveillance capitalism (Zuboff 2019), and platform surveillance (Murakami Wood and Monahan 2019). While immensely important, these data-centric approaches often overlook the nuance of quotidian operations under dataveillance afforded by the masking and relegating of responsibilities within the surveillants' digitized chains of command. Considering this, we map the ways in which the daily capabilities of agents implicated in a broader surveillance assemblage are expanded by making sweeping data-based capabilities not only *possible* but *convenient.* We do so through a thorough examination of a case study pertaining to the capabilities of a software deployed as part of the US border security apparatus.

To date, there have been few in-depth case studies of software used by the federal government and the associated implications of relying on Silicon Valley to build these technologies and, thereby, the nation's security systems. Often, the considerations are pragmatic: how does one get access, either through ethnographic or any other means, to the data generated at the intersection of those two notoriously closed worlds? In turn, we ask: how does ICM, a software product built by Palantir Technologies, function within the larger interfacial regime that is the United States' securitization apparatus? To answer this question by bypassing the de-facto impossible requirement of observing the deployment of the software or accessing those using it, we use the concept of interfacial regimes within the existing work on dataveillance and surveillant assemblages. First, we define and expand the notion to explain our theoretical groundwork. Next, we conduct a qualitative document analysis to systematically evaluate governmental, journalistic, and non-governmental sources (Bowen 2009). In turn, we visualize ICM's known information sharing flows with an interfacial regime map, thus identifying and organizing the many other databases and software programs ICM links to or interfaces with. This effort qualitatively evaluates the types of information ICM accesses, as well as analyzes the impact such access may have on the civil liberties of the individuals whose data are stored within ICM. This visualization serves as an important contribution to both the fields of software and surveillance studies in that it illustrates how people (and their associated identity records) are treated within a largely opaque and obscure surveillance infrastructure. We argue that ICM serves as an interfacial keystone within the United States' securitization apparatus and affords federal immigration agents significant power in governing immigration outcomes.

Interfacial Regimes, Surveillant Assemblages, and Control

What is an interface? To Bratton (2015: 241), interfaces are "any point of contact between two complex systems." But interfaces exist in dimensions far more complex than any physical "point" of contact; rather, we can understand this point as a "point of transition between different mediatic layers within any nested system" (Galloway 2012: 31). In the perspective that Alexander Galloway (2012: 33) articulates, interfaces are not tangible, objective things or static planes, but are instead effects because of their function to translate,

mediate, and process information from one significant material to another. Put simply, interfaces are not only the points of contact that we, as users, may interact with to access a complex system, such as the touchscreen of an iPhone. They also exist as an effect that mediates meaning between systems and drives interaction continuously rather than at static points of contact.

Interfaces have significant power in organizing the range of possible actions a user may take. In examining their physical nature, Bratton (2015: 221) argues that interfaces serve as "technical information machines" that work to clarify complex systems, such as computational algorithmic software, so that human users may interpret and use those complex systems. Moreover, Bratton (2015: 245) posits that the amalgamation of interfaces in our modern world works in synchrony to create "interfacial regimes" that enforce a "totalizing worldview." In other words, as interfaces *interface*, such as when complex databases interlink, the ability for this assemblage of interfaces to determine what is relevant or available to the human user at one end of the chain can significantly impact how that user interacts with the world. Murakami Wood and Monahan (2019: 2) note that Bratton espouses a "maximalist understanding" of the notion of platforms' power and call for a more grounded approach, rooted in the communal, rather than the abstract, ways in which people cooperate in digital technology. In this article, we use the word *interface* to denote the complex chains of potential actions afforded by the overall design of both back- and front-end components of a given system (Ash et al. 2018), rather than the more colloquial understanding of the graphic user interface (GUI) on-screen elements or the input/output methods by which such are accessed. Consequently, we are primarily interested in the interfacings of various elements of the ICM network and the way that this software allows the agents operating through the interlocking interfaces to conceive and operationalize humans via interlocking data-doubles.

The theoretical notion of assemblages and interfacings has a rich history within surveillance studies. In drawing from Deleuze and Guattari's (1987) definition of "assemblages," Haggerty and Ericson (2000: 609) note that modern surveillance systems, particularly those of government institutions, have coalesced so that they operate as surveillant assemblages. In this vein, surveillant assemblages are comprised of intertwined systems and technologies that function in unison to monitor, which in turn provides "for exponential increases in the degree of surveillance capacity" (Haggerty and Ericson 2000: 610). By increasing potential surveillance capacities, then, the very nature of contemporary surveillance has changed (Lyon 2007: 56) to incorporate chains of human and non-human actors exerting power (Latour 2005). The tendency to integrate surveillant technologies and computer networks has prompted a shift towards "dataveillance," or the "systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" (Clarke 1988: 499). Moreover, in recent years, such dataveillance has become increasingly automated. As commonly reported in scholarship and media, this trend is worrisome not only through intentional (mis)use of user data but also through a gradual erosion of conscious actions with regards to conducting or being subjected to surveillance and potentially accepting indiscriminate massive data collection as the "default" state. In this vein, one may be able to conduct deeper surveillance simply by virtue of availability and—perhaps more importantly—accessibility to vast troves of automatically collected data. As Andrejevic (2019: 2) poignantly warns, "data collection on this scale initiates a *cascading* logic of automation… While it is true that not all forms of information collection qualify as 'surveillance', the development of this sensor-permeated infrastructure enables new logics of surveillance to emerge and take hold" (emphasis in the original). As we show in the following qualitative analysis, an example of such a cascading effect can be seen in the way that multiple complementary databases are available to border agents without any impediment. This is a design choice of reducing the *friction* within a computerized system (Ash et al. 2018), which may lead to additional measures being taken against a target simply because they are available to the user.

Furthermore, this fundamental shift towards dataveillance has transformed how individuals are identified by the various surveillant assemblages that monitor them. As Haggerty and Ericson (2000: 611) note, the human body within a surveillant assemblage is effectively removed from its physical territorial setting and further "decorporealized," forming a so-called "'data double' of pure virtuality." This conceptualization is foreshadowed by Deleuze's notion of "dividuals" as articulated in his 1992 "Postscript on the Societies of

Control." In his analysis of modern "societies of control," Deleuze (1992: 4) argues that power governs the behaviors of "dividuals" whose identities and actions are infinitely divisible and may be reduced to data points by modern technology. In this sense, as modern technology becomes more ubiquitous and essential, so too does the "segmentation and rationalization of minute gestures within daily life," thus facilitating digital representations of humanity's complexity through series of encoded and interrelated data points (Galloway 2012: 92). Such representational capacity leads Galloway (Ibid.) to suggest that "the point of power today resides in networks, computers, algorithms, information and data." In this vein, we can understand interfaces and the interfacial assemblages of networks, computers, algorithms, information, and data as the "point of power" of which Galloway speaks.

Dividualization in Modern US Securitization

After the terrorist attacks of September 11, 2001 (9/11), in the United States, a heightened political climate and the threat of imminent demise prompted tremendous reforms to modernize the American security apparatus. President George W. Bush created the Department of Homeland Security (DHS) in 2002 with the mission to "create a border of the future" and oversee "a layered management system" that would increase the government's visibility of "vehicles, people and goods," (Office of Homeland Security 2002: 22). This process of securing the homeland would undoubtedly be expensive, and "billions of dollars awaited contractors who promised infallible new technology" (Brill 2016). According to a May 2018 report published by The Stimson Center, a nonpartisan policy research center specializing in security analysis, at least $2.8 trillion was spent on counterterrorism related efforts between 2002 and 2017 (Heeley et al. 2018: 5). And while industry veterans such as Boeing, Lockheed Martin, and Northrop Grumman quickly set out to win contracts, so too did Silicon Valley technology giants such as Amazon, Google, and Palantir Technologies (Mattern 2018).

While the country's security architecture undoubtedly needed an update, scholars have argued that private contractors and consultants purposefully exploited an environment of fear to sell technology with little consideration of their products' potential consequences. As Amoore (2011: 338) notes, "the discursive deployment of 'risk', particularly by management consultants" in the immediate aftermath of 9/11 spurred the politicization and securitization of everyday life through technology. This sentiment is echoed by David Lyon (2010), who notes that American policy makers usually revere technology despite lacking a complete understanding of its societal impacts. By turning to private industry to build America's modern security apparatus, securitization was never treated as a political issue but rather as a technical problem that could only be solved by "the power of the best minds of the private sector" (Amoore 2011: 345). In turn, private contractors have effectively developed, built, and maintained the country's current surveillance and technological security infrastructures.

Furthermore, securitization efforts facilitated by the rapid adoption of private industry technology after 9/11 demonstrate a distinct shift in strategy in which surveillance technology infrastructures create a means of "social sorting" and, in turn, anticipate and mitigate security threats (Lyon 2010: 22). In this sense, networked technologies have aided security and border officials by allowing them to mine external databases and develop complex data representations of individuals (Lyon 2010: 23; Amoore 2006). Amoore (2006: 27) argues that the United States' dependence on biometric technology, data mining software, and algorithmic applications in border security has resulted in the creation of the "data derivative," akin to Deleuze's (1992) concept of the dividual as well as Haggerty and Ericson's (2000) notion of the data double. The data derivative is an abstracted conception of a person based on data points aggregated from various securitization technologies that border security administrators then use to assign "risk groupings" to individuals (Amoore 2006: 27). In doing so, border security agents are "dividing, separating, and particularizing subjects" based on derived data from surveillance technologies, biometric data, and other personal details (Amoore 2006: 35). The preemptive deployment of surveillance technologies based on the social sorting of data derivatives thus "renders data actionable" in that it permits officials to model and predict perceived threats before they materialize (Amoore 2006: 29; Andrejevic 2019).

In addition to the increased appetite for surveillance technologies in the post 9/11 security environment, loud calls for uninhibited information sharing between agencies largely ignored the privacy ramifications of implementing systems and security architectures of mass surveillance. In one such justification for data mining and information sharing, Lee Strickland and Jennifer Willard (2002: 16) carelessly ask, "Why would we not resort to the abundance of extant information that is compiled daily on individuals in our global economy in this information age?" Indeed, as Lyon (2007: 56) notes, the urgent declaration of a "war on terror" effectively validated calls for the uninhibited expansion of integrated and automated surveillant assemblages. Together, the use of surveillance technology as a mechanism to socially sort and categorize individuals according to their threat level and the unrestricted information sharing practices indicative in the aftermath of 9/11 marked a distinct new phase in America's security apparatus.

This process of dividing, separating, and particularizing "subjects" can substantially impact how a person is governed and treated should he or she try to cross a border. It is this governing capacity of algorithms and software products when used in the context of a security apparatus that prompts Amoore (2006: 35) to ask, "What are the implications of visualizing subjects in this way?" Mattern (2018) echoes this concern in her critical analysis of recognition software deployed at the US southern border, suggesting that people who approach the border are dehumanized by the assemblage of securitization interfaces that incessantly gather data on them. Rather than being viewed as human beings, border crossers are "discussed as 'movements' or 'flows'; or, simply, 'items of interest'" (Mattern 2018). This trifecta—the derivation of human identity from data points, the use of algorithms to identify those who "belong," and the dehumanizing capacity of technology—considerably impact an individual's mobility, the extent to which they are surveilled, and how they are governed as a "target" by the various federal US agencies whose databases they exist in. And, while Amoore (2006) and Mattern (2018) hold the singular system in the crosshairs of their critique, the situation becomes ever so complicated when multiple interlocking systems are at play. Professing a Brattonian interfacility, users of such systems (be it government agents or border officials) enter an even more asymmetrical relation with their "targets" as those targets are being black boxed, dividualized, and repackaged by successive algorithmic systems. Each such transition is a cumulative "effect" and, viewed from a nonrepresentational perspective, engenders additional limitations on the way people are viewed within the US border surveillance assemblage.

Palantir Technologies and Investigative Case Management

Palantir, founded in 2004, is a company that develops and sells data mining and analysis software. Palantir is privately owned by its founders, who include PayPal founder Peter Thiel, and received a $20 billion valuation in its latest fundraising round in 2015 (Munn 2017). While the company has worked diligently to publicize itself as a Washington outsider, Palantir has quietly amassed US government contracts worth more than $1.2 billion since 2009 (Mitchell 2016). In fact, Palantir was first established with $2 million in seed funding from the Central Intelligence Agency's (CIA) venture capital arm In-Q-Tel, setting the company on the path of collaborating with the federal government for years to come (Mitchell 2016).

Palantir's relationship with Immigration and Customs Enforcement (ICE), a department within DHS, is of particular interest considering the agency's increased reliance on Palantir software. ICE currently uses a plethora of Palantir developed products, including the data analysis platform Gotham, a database and analytical platform called FALCON, and an analysis software dubbed the Analytical Framework for Intelligence (AFI), which is considered to be "the black box system of profiling algorithms" that supports President Trump's "extreme vetting" of immigrants initiative (Mijente, The National Immigration Project, and Immigrant Defense Project 2018: 32; Woodman 2017). Yet the most influential software used by ICE is Palantir's Investigative Case Management (ICM) platform, which the DHS purchased for $53.1 million in September 2014 (Mijente, The National Immigration Project, and Immigrant Defense Project 2018: 32). ICM enables immigration agents to retrieve and aggregate data, such as an individual's biometric data, personal relationships, and criminal history, by interfacing with multiple other databases. This not only includes databases within the DHS but also with other federal, state, and local agencies as well as commercial databases (Mijente, The National Immigration Project, and Immigrant Defense Project 2018: 32). In turn, this amalgamation of information is used to build detailed profiles on preemptively dividualized

"targets" (Woodman 2017). While ICM has become the primary tool used by ICE to facilitate deportations, funding documents from DHS reveal that "US Citizens are still subject to criminal prosecution and thus are a part of ICM" (Woodman 2017). In this sense, both American citizens and foreign nationals are within the realm of ICM's tentacled data gathering and analyzing processes.

Palantir has not escaped criticism for its allegedly benevolent mission to help humanitarian and government bodies in managing and leveraging data for increased efficiency. In early February 2019, Palantir announced a partnership with the United Nations World Food Program (WFP) in which the company would provide software and data mining support to help cut costs and better serve WFP's 92 million aid recipients, or "customers," as Palantir executive vice president Josh Harris called them (Parker 2019). Privacy groups and advocates for responsible data use expressed immediate alarm at the partnership, pointing to the risks associated with Palantir accessing WFP's recipient data to build algorithmic models and the lack of transparency, accountability, and oversight the partnership is subject to (Responsible Data 2019).

Palantir has also been critiqued for providing free predictive policing software to the New Orleans Police Department (NOPD) (Winston 2018). The Palantir and NOPD partnership never went through a public procurement process, thus leading many to question why the partnership had been kept secret (Winston 2018). Indeed, predictive policing software has been widely decried as inaccurate and discriminatory because its algorithms are trained using biased policing data (Lum and Isaac 2016: 15). However, that has not prevented other city police departments, including New York City and Los Angeles, from purchasing and deploying Palantir's predictive analytics software for law enforcement purposes (Winston 2018; Munn 2017).

Palantir plays a significant role in the development and implementation of many essential technology infrastructures within the public sector. Yet, while Palantir's software suite has been used by engineering and computer science scholars to study emerging analytic technological capabilities (see, for example, Wright et al. 2009 and Yu et al. 2014), the company's software products have received limited academic critique from a sociological or humanities perspective. In this sense, Palantir's sophisticated technologies operate rather opaquely, and the functionality and scope of these technologies, such as ICM, is largely unknown to both users of the software and scholars who seek to study the effects such software has on people's lived experiences. Thus, we present the following qualitative research protocol as an attempt at understanding ICM's integration into America's contemporary surveillance and securitization infrastructures.

Visualizing ICM's Interfaciality

To understand how ICM functions within the larger interfacial regime that is the United States' securitization apparatus, we designed a visual representation in the form of an interfacial regime map. It attempts to illustrate the largely unrecognized information sharing practices that provide ICM, and thereby ICE agents, with significant access to an immigrant's personal data which can, in turn, be used to govern his or her immigration outcome. As Bratton (2015: 241) notes, information visualization is a means of design that attempts to articulate the interfacial chains "so that their form might be grasped." At the same time, representing information flows visually is inherently reductive; any attempt to summarize "planetary scale computational networks" for conceptual digestion immediately minimizes a system's complexity (Bratton 2015: 231). Considering these constraints, this ICM interfacial regime map must be understood not as an all-encompassing depiction but as a simplified, single layer representation of ICM's interfacings and information aggregation methods.

Due to the confidential nature of the DHS's operations, little information about ICM is publicly available. The primary resource that informed the design of this interfacial regime map was the ICM Privacy Impact Assessment (PIA), published on June 16, 2016 by the DHS (Neuman 2016). The PIA is a legally mandated assessment of ICM's privacy protection measures and "interrelated capabilities," meaning its capacity to interface and extract data from various resources (Neuman 2016: 1). We also utilized investigative reporting

by Spencer Woodman, a journalist with The Intercept, which is an internationally acclaimed news organization (Woodman 2017). Finally, this interfacial regime map is informed by data gathered from an investigative report commissioned by Mijente, the National Immigration Project, and the Immigrant Defense Fund (2018), which reveals the DHS's various connections to Silicon Valley and with Palantir in particular. Other supporting public documents from the original request for proposals for ICM were used to cross reference statements in the Privacy Impact Assessment (Neuman 2016). These include the TECS Modernization Program Operational Requirements Document (US Immigration and Customs Enforcement 2014a), the ICM Statement of Objectives (US Immigration and Customs Enforcement 2014b), and the High Level Technical and Mission Requirements Matrix (US Immigration and Customs Enforcement 2014c). These documents were obtained from the Federal Business Opportunities website (www.fbo.gov) by searching for the project solicitation number (HSCETC-14-R-00002) and from The Intercept's investigative reporting.

To analyze these sources, we employed a qualitative document analysis approach, which is particularly useful for intensive case studies that seek to investigate a single phenomenon, object, or program (Bowen 2009: 29). While conducting close readings of the documents, we categorized in a spreadsheet all mentions of various digital objects—databases, networks, systems, and software products—with which ICM interfaces. We primarily relied upon the PIA for this, as it was the most recently published public document and provided the greatest level of detail on ICM's interfacings. We organized those digital objects by category (government or commercial), the information sharing type (inbound to ICM, outbound from ICM, or bi-directional), the agency/owner and sub-agency (such as the Department of Justice or the Federal Bureau of Investigations), and, finally, the type of information provided. Finally, we used these findings to design the ICM interfacial regime map in Adobe Illustrator.

A total of twenty-one interfacing objects were identified as part of the ICM interfacial regime. ICM interfaces predominantly with other databases owned by the DHS, especially those also managed by ICE. ICM interfaces with four databases owned by the Department of Justice (DOJ) and with one database owned by the Department of State (DOS). Finally, this analysis revealed that ICM interfaces with a handful of nongovernmental databases and commercial resources. The full list of interfaces is available in Appendix 1 at https://doi.org/10.21942/uva.12315209.v1.

Information Sharing Types

ICM's primary function is to aggregate information from external databases, as evidenced by the dominant role inbound information plays in the ICM interfacial regime. In total, fourteen of the twenty-one databases ICM interfaces with provide it with information, and many of these databases are accessible from within ICM itself (Neuman 2016: 5). This means that a user can query and automatically import or access information from an external database without ever leaving the ICM interface. According to the ICM PIA, the following seven databases are accessible from within ICM's interface, as shown in Table 1.

Database	**Information Accessible**	**Agency/ Sub-agency**
ATS (Automated Targeting System)	ICM users may query ATS from within ICM for information on passengers, vehicle or aircraft border crossings, secondary investigation logs, visa and passport data, and other information relevant to investigations and manually copy any pertinent data into subject records or case documents.	DHS/CBP
EID (Enforcement Integrated Database)	ICM users may access EID arrest data. EID arrests are primarily made by HSI or ERO. Within ICM, a user may query EID for an individual and if that individual's record is found, the user can pull all information collected on that	DHS/ICE

	individual contained in EID into ICM.	
FALCON-DARTTS (FALCON Data Analysis & Research for Trade Transparency System)	ICM can search FALCON-DARTTS from within the ICM application. FALCON-DARTTS contains information on Financial Crimes Enforcement Network data, currency and monetary instrument reports, currency transaction reports, suspicious activity reports, reports relating to coins and currency received in nonfinancial trade or business, reports of foreign bank, and financial accounts.	DHS/ICE
NCIC (National Crime Information Center)	ICM users may query NCIC from within ICM via ICE's existing connection to NCIC. This connection is housed within ICE's Alien Criminal Response Information System (ACRIMe). NCIC contains information on criminal targets, immigration violators, stolen articles, warrants, terrorist watchlist records, state and federal criminal history reports, and reports of missing persons.	DOJ/FBI
SEACATS (Seized Assets and Cases Tracking System)	ICM users may query SEACATS from within ICM to obtain records of seizures of contraband. This usually occurs when an ICM user is creating a seizure report within a case. The user can directly import the data from SEACATS into the seizure report. Information from SEACATS may also be manually input into other case documents, such as ROIs or arrest reports.	DHS/CBP
SEVIS (Student and Exchange Visitor Information System)	ICM users may search SEVIS from within ICM and either directly import or manually copy SEVIS data into a case record. SEVIS contains biographic and immigration status data about individuals who are temporarily admitted to the United States as students or exchange visitors.	DHS/ICE
TECS (Treasury Enforcement Communications System)	ICM users may query TECS from within ICM for information related to any person associated with a case. This includes subject records, border crossings, and inspection records. TECS is the legacy case management system used by CBP; use of TECS was scheduled to end by September 30, 2015.	DHS/CBP

***Table 1**: Databases ICM users may access from within ICM itself.*

ICM also pushes information outward, primarily via the Law Enforcement Information Sharing Service (LEIS Service). Through the LEIS Service, which is owned and operated by ICE, external federal, state, local, regional, and international law enforcement agencies can access unclassified information. While relatively little has been published about the LEIS Service, the Mijente report notes that this outward information sharing practice is a focal point of the DHS's efforts to communicate with domestic law enforcement officials, especially those along the southern US border (Mijente, The National Immigration Project, and Immigrant Defense Project 2018: 45).

Information Collected/Provided

By connecting with twenty-one different interfaces, ICM collects a wealth of detailed information. According to the ICM PIA, this information is divided into six categories: biographic data, descriptive data, financial data, evidence and descriptions of evidence obtained during an investigation, location-related data,

and telecommunications data (Neuman 2016: 9-12). Table 2 below includes a sampling of information from each category.

Biographic data	• Target name • Date of birth • Social Security Number • Alien Registration Number • Address • Driver's license number • Passport number • Criminal history • Immigration status and history
Descriptive data	• Eye color • Hair color • Height • Weight • Scars, marks, tattoos
Financial data	• Suspicious financial activity • Currency transaction reports • Currency and/or monetary instrument reports
Evidence and descriptions of evidence obtained during an investigation	• Statements of targets/witnesses • Photographs • Emails • Banking records • Travel history records • "Other related documents" such as videos, audio, maps, or other visual representations of information
Location-related data	• Data gathered from "location tracking tools," such as mobile phone triangulation • License plate reader data
Telecommunications data	• Telecommunication device identifiers: phone numbers, International Mobile Subscriber Identity, email addresses, and IP addresses • Telecommunications usage data: date/time, duration, dialed number, originating and terminating cell tower locations • Biographic information on targets of investigations, potential targets, associates of targets, or any individuals or entities that receive calls from these individuals

Table 2: *A sampling of information and data collected and provided on ICM "subjects."*

Based on our findings, this interfacial regime map (Figure 1) is an attempt to visualize how ICM functions within the larger US information technology security apparatus. The map offers a simplified view of the ICM interfacial assemblage with regards to (1) the departments and sub-agencies that link to ICM (distinguished by color, shape, and position of the polygon); (2) additional national, international, and commercial actors; and (3) the type of data flows that occur between them (inbound, outbound, or bi-directional).

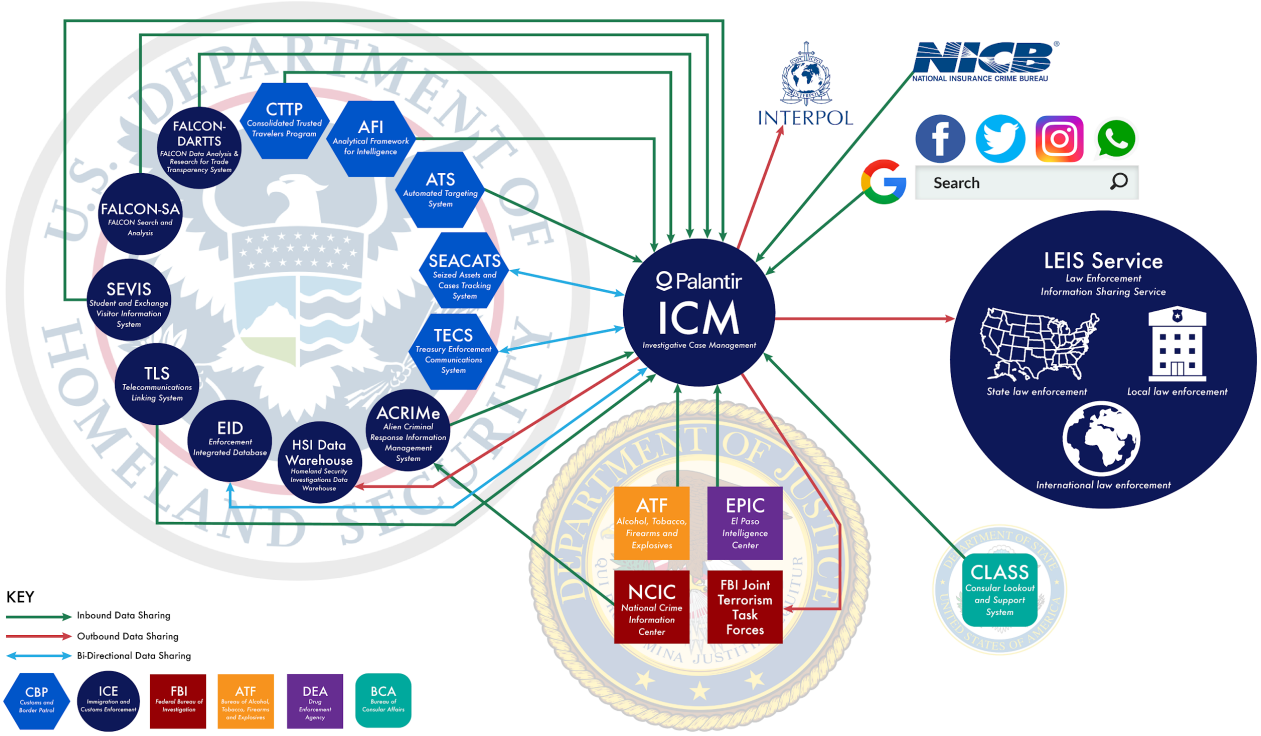

Figure 1: *The ICM Interfacial Regime Map. (Available in higher resolution as* Appendix 2 *at https://doi.org/10.21942/uva.12315218.v1), design: Emma Knight*

ICM's Governing Capacity in America's Immigration System

ICM functions as an aggregating and centralizing force within America's security apparatus. Moreover, access to ICM enables its users, specifically immigration officials involved in deportation proceedings, to wield significant control over the "targets" whose identities are formed from the data ICM obtains. The lack of publicly available documentation on ICM, as well as the contradictory information these public documents often offer, provide significant reason for concern about the governing and surveillant power this software product holds.

To begin, the scope of ICM's purpose has shifted substantially since the project was proposed in February 2014. According to the Statement of Objectives, ICM was originally intended for use solely by the office of Homeland Security Investigations (HSI) for criminal law enforcement actions (US Immigration and Customs Enforcement 2014b: 2). However, the PIA published two years later reveals that the office of Enforcement and Removal Operations (ERO) now relies on ICM for civil immigration enforcement and deportation in addition to criminal enforcement (Neuman 2016: 1).

This broadened scope aligns with efforts by both the Obama and Trump administrations to increase deportations of undocumented immigrants. Particularly under the Trump administration, ICE has demonstrated great eagerness in conducting large scale immigration raids, and President Trump has repeatedly claimed that ICE will arrest and deport "millions" of noncriminal undocumented immigrant families in 2019 (Mijente, The National Immigration Project, and Immigrant Defense Project 2018: 2; Miroff et al. 2019). Moreover, these raids have become increasingly pinpointed because of ICE's unrestricted access to information on immigrants and citizens alike. Between October 2017 and May 2018, half of all ICE raids were conducted in just twenty-four of the 3,142 counties in the United States (Misra

2018). ICM's unfettered access to personally identifiable data, location-based data, and telecommunications data has supported ICE's surveillant capacities and abilities to target noncriminal undocumented immigrants in raids. In effect, this is another example of Murakami Wood and Monahan's (2019: 1) "platform surveillance": while "the emergent forms of platform capitalism portend new governmentalities," this also means the traditional border security power structures come to rely on platform-like logics in the restructuring of their capacities. ICM can thus be read as the *platformization* of *traditional* surveillance.

The outbound flow of information from ICM to external federal, state, local, and international law enforcement agency partners via the LEIS Service is further evidence of the governing power ICM affords. By interfacing directly with ICM, LEIS directly distributes information to law enforcement agents across the country who can subsequently detain individuals on ICE's behalf (Mijente, The National Immigration Project, and Immigrant Defense Project 2018: 45). Even so-called "sanctuary cities" such as New York and San Francisco that refuse to cooperate with ICE in this manner have experienced heavier ICE presence in the Trump era (Mijente, The National Immigration Project, and Immigrant Defense Project 2018: 2). This is due in part to the detailed information ICE agents are able to obtain from ICM, which allows for greater accuracy when arresting individuals (Misra 2018). Even though undocumented immigrants are legally protected from unreasonable searches and seizures by the United States Constitution's Fourth Amendment, the highly specified information ICE officials have access to, down to a "target's" place of worship, have facilitated ICE crackdowns across the country (American Civil Liberties Union 2017: 6).

ICM's governing power, however, stems most deeply from its method of bulk and cumulative information aggregation that works to dehumanize individuals and reduce people to "targets," "subjects," and even "items of interest" whose identities are determined solely by an algorithmic assessment of interrelated data points (Mattern 2018). As Mattern (2018) notes, the technologies used to secure the United States' borders must "be understood in the context of the ideological regimes that control them." Analyzing the ICM interfacial regime as a surveillant assemblage and visualizing its deeply entrenched network of interfacings reveals the extent to which immigrants and citizens alike are reduced to "data derivatives" (Amoore 2011: 28), "data images" (Lyon 1994: 19), or "dividuals" (Deleuze 1992: 4). This reduction of human identity to "bits of data" is a hallmark of the modern surveillance state and can establish conditions for state institutional actors, such as ICE officials, to "believe that they, not data-subjects, 'own' personal data" (Lyon 1994: 99). By illustrating the known data flows and interfacings of ICM, we have attempted to make clear the potential power ICM, and thereby ICE immigration officials, possess to dehumanize the individuals ICM virtually represents. Moreover, we seek to visualize the typically obfuscated nature of surveillant assemblages with this interfacial regime map and situate ICM as a key component within America's broader interfacial regime of securitization.

Finally, this theoretical and visual analysis of ICM has sought to explore how ICM exemplifies the broader ethos of the post-9/11 securitization era in which privately-created technology has been embraced as a panacea and software has been designed to recognize human beings in terms of their risk assessment scores rather than their humanity. When private corporations like Palantir build the technological components of today's ubiquitous surveillant assemblages, the boundary between public and private ownership of surveillance, and thereby those under surveillance, is blurred (Lyon 1994: 100). If the democratic values of the United States are to be upheld and abuse of governance to be avoided, we must question and contest the interfacial regimes that support the US security system more broadly.

Glossary

CIA	Central Intelligence Agency
CBP	Customs and Border Patrol
DHS	Department of Homeland Security
DOJ	Department of Justice

DOS	Department of State
ERO	Enforcement and Removal Operations
FBI	Federal Bureau of Investigations
HSI	Homeland Security Investigations
ICE	Immigration and Customs Enforcement
ICM	Investigative Case Management
LEIS Service	Law Enforcement Information Sharing Service
PIA	Privacy Impact Assessment
UN WFP	United Nations World Food Program
9/11	Terrorist Attacks of September 11, 2001

References

American Civil Liberties Union. 2017. *Sanctuary Congregations and Harboring FAQ*. American Civil Liberties Union, March. https://www.nwirp.org/wp-content/uploads/2017/03/ACLU-Sanctuary-FAQ-March-2017.pdf [accessed December 21, 2018].

Amoore, Louise. 2006. Biometric Borders: Governing Mobilities in the War on Terror. *Political Geography* 25 (3): 336–51.

———. 2011. Data Derivatives: On the Emergence of a Security Risk Calculus for Our Times. *Theory, Culture & Society* 28 (6): 24–43.

Amoore, Louise, and Marieke De Goede. 2005. Governance, Risk and Dataveillance in the War on Terror. *Crime, Law and Social Change* 43 (2): 149–73.

Amoore, Louise, and Rita Raley. 2017. Securing with Algorithms: Knowledge, Decision, Sovereignty. *Security Dialogue* 48 (1): 3–10.

Andrejevic, Mark. 2019. Automating Surveillance. *Surveillance & Society* 17 (1/2): 7–13.

Ash, James, Ben Anderson, Rachel Gordon, and Paul Langley. 2018. Digital Interface Design and Power: Friction, Threshold, Transition. *Environment and Planning D: Society and Space* 36 (6): 1136–53.

Bowen, Glenn A. 2009. Document Analysis as a Qualitative Research Method. *Qualitative Research Journal* 9 (2): 27–40.

Bratton, Benjamin H. 2015. *The Stack: On Software and Sovereignty*. Cambridge, MA: MIT Press.

Brill, Steven. 2016. Is America Any Safer? *The Atlantic*, September. https://www.theatlantic.com/magazine/archive/2016/09/are-we-any-safer/492761/ [accessed December 21, 2018].

Clarke, Roger. 1988. Information Technology and Dataveillance. *Communications of the ACM* 31 (5): 498–512.

Deleuze, Gilles. 1992. Postscript on the Societies of Control. *October* 59: 3–7.

Deleuze, Gilles, and Félix Guattari. 1987. *A Thousand Plateaus: Capitalism and Schizophrenia*. Minneapolis, MN: University of Minnesota Press.

Galloway, Alexander R. 2012. *The Interface Effect*. Cambridge, UK: Polity.

Haggerty, Kevin, and Richard Ericson. 2000. The Surveillant Assemblage. *British Journal of Sociology* 51 (4): 605–22.

Heeley, Laicie, Amy Belasco, Mackenzie Eglen, Luke Hartig, Tina Jonas, Mike McCord, and John Mueller. 2018. Counterterrorism Spending: Protecting America While Promoting Efficiencies and Accountability. Stimson Study Group. Washington, D.C: The Stimson Center. https://www.stimson.org/sites/default/files/file-attachments/CT_Spending_Report_0.pdf [accessed July 8, 2019].

Johnson, Heather L. 2014. *Borders, Asylum and Global Non-Citizenship: The Other Side of the Fence*. Cambridge, UK: Cambridge University Press.

Latour, Bruno. 2005. *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford, UK: Oxford University Press.

Lum, Kristian, and William Isaac. 2016. To Predict and Serve? *Significance* 13 (5): 14–19.

Lyon, David. 1994. *The Electronic Eye: The Rise of the Surveillance Society*. Cambridge, UK: Polity.

———. 2007. *Surveillance Studies: An Overview*. Cambridge, UK: Polity Press.

———. 2010. Surveillance, Power and Everyday Life. In *Emerging Digital Spaces in Contemporary Society*, edited by Philip Kalantzis-Cope and Karim Gherab-Martín, 107–20. London, UK: Palgrave Macmillan UK.

———. 2015. *Surveillance After Snowden*. Cambridge, UK: Polity Press.

Mattern, Shannon. 2018. All Eyes on the Border. *Places Journal*, September.

Mijente, The National Immigration Project, and Immigrant Defense Project. 2018. Who's Behind ICE? The Tech and Data Companies Fueling Deportations. Empower, October. https://mijente.net/wp-content/uploads/2018/10/WHO'S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations_v3-.pdf [accessed July 8, 2019].

Miroff, Nick, Maria Sacchetti, Arelis R. Hernández, and Josh Dawsey. 2019. Fear of Immigration Raids Looms as Plans for ICE "Family Operation" Move Forward. *Washington Post*, July 6. https://www.washingtonpost.com/immigration/fear-of-immigration-raids-loom-as-plans-for-ice-family-operation-move-forward/2019/07/05/76788e2a-9f41-11e9-b27f-ed2942f73d70_story.html [accessed July 8, 2019].

Misra, Tanvi. 2018. The Stark Geography of U.S. Immigration Raids. *CityLab*, October 25. https://www.citylab.com/equity/2018/10/where-ice-immigration-raids-are-concentrated/573883/ [accessed December 20, 2018].

Mitchell, Ellen. 2016. How Silicon Valley's Palantir Wired Washington. *POLITICO*, August 14. https://www.politico.com/story/2016/08/palantir-defense-contracts-lobbyists-226969 [accessed December 20, 2018].

Munn, Luke. 2017. "Seeing with Software: Palantir and the Regulation of Life. *Studies In Control Societies* 2 (1).

Murakami Wood, David, and Torin Monahan. 2019. Editorial: Platform Surveillance. *Surveillance & Society* 17 (1/2): 1–6.

Neuman, Karen. 2016. *Privacy Impact Assessment for ICE Investigative Case Management DHS/ICE/PIA-045*. Washington, DC: Department of Homeland Security. https://www.dhs.gov/publication/dhs-ice-pia-045-ice-investigative-case-management [accessed July 8, 2019].

Office of Homeland Security. 2002. *National Strategy for Homeland Security*. Washington, DC: Office of Homeland Security. https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf [accessed July 8, 2019].

Parker, Ben. 2019. New UN Deal with Data Mining Firm Palantir Raises Protection Concerns. *The New Humanitarian*, February 5. https://www.thenewhumanitarian.org/news/2019/02/05/un-palantir-deal-data-mining-protection-concerns-wfp [accessed July 8, 2019].

Responsible Data. 2019. Open Letter to WFP Re: Palantir Agreement. *Responsible Data* (blog), February 8. https://responsibledata.io/2019/02/08/open-letter-to-wfp-re-palantir-agreement/ [accessed July 8, 2019].

Strickland, Lee, and Jennifer Willard. 2002. Re-Engineering the Immigration System: A Case for Data Mining and Information Assurance to Enhance Homeland Security Part 1: Identifying the Current Problems. *Bulletin of the American Society for Information Science and Technology* October: 16–21.

US Immigration and Customs Enforcement. 2014a. ICE TECS Modernization Program Operational Requirements Document (ORD). Washington, D.C: US Department of Homeland Security. https://theintercept.com/document/2017/03/02/ice-tecs-modernization-operational-requirements/ [accessed July 8, 2019].

———. 2014b. Immigration and Customs Enforcement (ICE) TECS Investigative Case Management (ICM) Statement of Objectives. Washington, D.C: US Department of Homeland Security. https://theintercept.com/document/2017/03/02/ice-icm-statement-of-objectives/ [accessed July 8, 2019].

———. 2014c. High Level Mission and Technical Requirements, Solicitation HSCETC-14-R-00002. US Department of Homeland Security. https://www.fbo.gov/index?s=opportunity&mode=form&id=36fb3b697a2ccb4ec7084b4e0ec6cdb9&tab=core&_cview=1 [accessed July 8, 2019].

Van Dijck, Jose. 2014. Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology. *Surveillance & Society* 12 (2): 197–208.

Winston, Ali. 2018. Palantir Has Secretly Been Using New Orleans to Test Its Predictive Policing Technology. *The Verge*, February 27. https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd [accessed February 12, 2019].

Woodman, Spencer. 2017. Palantir Provides the Engine for Donald Trump's Deportation Machine. *The Intercept*, March 2. https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/ [accessed December 20, 2018].

Wright, Brandon, Jason Payne, Matthew Steckman, and Scott Stevson. 2009. Palantir: A Visualization Platform for Real-World Analysis. In *2009 IEEE Symposium on Visual Analytics Science and Technology*, 249–50. Atlantic City, NJ: IEEE.

Yu, Ze, Min Li, Xin Yang, and Xiaolin Li. 2014. Palantir: Reseizing Network Proximity in Large-Scale Distributed Computing Frameworks Using SDN. In *2014 IEEE 7th International Conference on Cloud Computing*, 440–47. Anchorage, AK: IEEE.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power*. London, UK: Profile Books.