# Data as Ammunition – A New Framework for Information Warfare

Lt. Col. Jessica Dawson, Ph.D.
Col. Katie Matthew, Ph.D.

## ABSTRACT

*This article presents a new framework for thinking about data and the risks posed to national security. Taking issue with the prevailing analogy of "data as oil," this article argues that viewing data as ammunition provides a clearer understanding of the real threats and a familiar path toward risk mitigation in the information space. The "data as ammunition" analogy carries a better intuitive depiction of the risk and why, in the days of increasing storage which keeps data easily accessible seemingly forever, categorizing data through the lens of ordnance classifications can help clarify the risks to force and national security. We close this article with recommendations to adapt current privacy, security, and commercial policies to mitigate the new risks to force and personnel on and off the battlefield.*

***Keywords:*** *Data, Analytics, Publicly Available Information, Micro-Targeting, Information Domain*

## INTRODUCTION: EXPLAINING INFORMATION WARFARE IN WARFARE TERMS

This article expands on the definition of data and data information in the Army's newest doctrine ADP 3-13 and advances a new framework for thinking about data and the risk posed to national security. We lay out how and why thinking about how the definitions in ADP 3-13 are a vast improvement in the Army's doctrinal understanding of data but that defining the interpretation data as "receiver centric" does not go far enough in setting up frameworks for *understanding the impact* of varying interpretations of data. If we categorize data as ammunition, we move it from the academic or doctrinal realm of "meaning of information" and into a more military focused national


**Lieutenant Colonel Jessica Dawson** is a United States Military Academy professor in the Army Cyber Institute and is the Digital Force Protection Research Team Division Chief. She has written numerous articles about the risks of commercial data collection and has advised senior leaders across the federal government on these risks. She holds a Ph.D. in sociology from Duke University.

defense arena – after all, ammunition literally has impact and we argue, so does data. By thinking about data as ammunition, we argue we start to think of the impact of the data on people and society. This new framework is necessary to combat the buzzwordification of data, which prevents deeper understanding and application of the concept and uses an analogy familiar to most military personnel to describe data. The Army does not need leaders who ask for "big data" – they need to understand what problem they are asking data to solve. Ammunition, we argue, is a better framework for understanding what data can do and this shift is necessary to help the Army better understand this major shift in the character of war. Treating data as ammunition reduces the tendency of leaders to store data for data's sake and instead recognizes the potential impacts on individuals and the force.

## BACKGROUND: HOW WAR AND PERSONAL DEVICES CHANGED WEAPONS

When one of the first Americans serving in Iraq died in an explosion on May 26, 2003 – only six weeks after the initial U.S. invasion had "ended" – the U.S. military had no words to describe the type of ordnance that exploded under his vehicle and killed him.[1] The device that killed Private First-Class Jeremiah Smith came to be known as an improvised explosive device (IED) and was not a new concept in warfare. The French Resistance, for example, used IEDs extensively to derail the German supply lines during World War II, and with the massive amount of discarded and leftover ordnance lying around Iraq and the number of unemployed former soldiers who knew how to use it, Iraq became a war of IEDs.

What the U.S. military learned early on was that commercial, off-the-shelf technology could easily be repurposed to make the already deadly IEDs even more precise and more lethal. Iraqi insurgents and technology evolved together, and IEDs and the mechanisms

**Colonel Katie E. Matthew**, U.S. Army, is a United States Military Academy professor in the Department of Behavioral Sciences and Leadership. She has served as a logistician at home and on deployment with the 1st Theater Sustainment Command, 1st Infantry Division, 82nd Airborne Division, and Joint Special Operations Command, and most recently commanded the Brigade Special Troops Battalion and Camp Buehring, U.S. Army Central Command. She holds a Ph.D. in sociology from George Mason University.

and methods used to detonate them, grew more sophisticated. Over time, IEDs shifted from needing a vehicle or victim to detonate to having wired or remote detonation capabilities – often done by cell phone. Suddenly, once mundane activities – using a cell phone – became threatening, and allied troops had to determine if the civilian seen holding a cell phone was either a lethal threat to the force or someone simply using their phone for its intended purpose – a notion that seemed absurd before cell phones became detonators.

In many ways, the cell phones that millions carry with them continue to have dual potential: a loaded weapon and a useful device to store data. The data that each of us has to hand to aid in our daily lives also opens a vulnerability to the force as a new form of ammunition on and off the modern battlefield.[2] Just as IEDs were adapted to be able to target different size formations, data can be used to do wide area targeting or precision microtargeting,[3] but the end state is the same: soldiers are removed from the fight. We argue that thinking about data as ammunition helps leaders to better understand and comprehend the impact on the force, viewing it as a tool in a broader arsenal.[4]

## A BAD ANALOGY: THE LIMITATIONS OF DATA AS OIL

There are many analogies about data in modern society, but none is as pervasive as "data is the new oil."[5] Originally coined in *The Economist* in 2017, the analogy describes data as something that can be traded, bartered, owned, or stolen—as something whose value underwrites the entire digital economy. The data as oil analogy conceals many of the risks from the new data economy. ADP 3-13 defines data as "any signal or observation from the environment"[6] but the broader societal discussion of data is more informative for defining the problem we are addressing. The "data as oil" analogy also works to prevent and limit regulation, as viewing something as a commercial

commodity makes it more difficult to quantify as dangerous and yet, considerations of risk associated with data are not new.[7] Viewing data as a commodity also falsely leads to the idea that that more data is better; in reality, more data is simply *more*. This analogy also creates difficulties for privacy advocates who struggle to demonstrate how data can be weaponized against individuals[8] when their arguments are outweighed by the commercial interest of those that depend on data for financial interests, which in turn influence the national conversation around the risks from data. Army leaders are not immune to absorbing these ideas and this makes it more difficult for them to conceptualize data as something that can be used against them or the force. It is difficult for everyday people to understand how something they do on their phone can be turned into data that can be used against them. This is also where one of several major myths about data and privacy from the commercial surveillance economy come into play: if you have nothing to hide, what are you worried about?

Ammunition, like data, can be used for good things like providing food or protection. Ammunition can also be destructive, just as the cell phone in Iraq could be a completely harmless device or a detonator for a mass casualty event. All military equipment and ammunition are classified according to a federal supply classification (FSC).[9] Most ammunition, apart from nuclear associated ammunition, is classified as FSC Group 13 and it is categorized according to the size of the projectile and stored according to its potential risks. We argue that moving data from the generic conception of information to categorizing it in terms of its effects would significantly move the discussion on how to protect it more effectively both from a DoD perspective and a broader national security perspective.

From a practitioner perspective, the "data as ammunition" analogy carries a better intuitive depiction of the risk from varying interpretations of data, particularly for those who are less steeped in data expertise. In the days of increasing storage which keeps data easily accessible seemingly forever (though this is currently in doubt),[10] new ways of thinking about data are necessary. For example, thinking of data as a minefield subject to algorithmic overwatch helps better define the risks, not only to individuals but to the force and national security writ large. Categorizing data through the lens of ordnance classifications (i.e. different types of ammunition) can help clarify and quantify the risks to force and national security, both for staff and commanders as well as other decision makers such as contracting officers. If the use of data comes from the interpretation of it, then decision-makers must be aware of how different interpretations of the data can be used to attack red or attack blue – just like ammunition.

## A BETTER (NOT ABSOLUTE) ANALOGY: DATA AS AMMUNITION

Why do we argue that we should use an analogy of data as ammunition? Analogies can be useful in thinking about complicated topics and, there are not many more confusing topics – for a variety of reasons – than data. In the rush to obtain more data, industry leaders have focused on the potential opportunities and paid less attention to the risks. Treating data as

ammunition through its dual potential better prepares military leaders and lawmakers on how to safeguard, manage, and appropriately utilize data.

Storage of ammunition is based on the caliber and potential damage. Where data is similar is that very innocuous data can be combined and enriched to create much more powerful impacts on individuals or at scale. We currently segregate many things based on the risk they create when they are combined. We store bleach and ammonia separately. We segregate knowledge to those who have a need to know. Data should be no different – leaders need to know what data they need to answer particular questions. Simply demanding more data is like demanding more ammunition without considering what you are trying to use said ammunition for.

## FROM DATA BUZZ WORDS TO DATA LITERACY

Data, like ammunition, is meaningless without the proper tools and interpretations. Analytics or interpretations of the data are necessary to get any use out of data. Information warfare and information advantage imply putting data into use as tools. It is relatively easy to understand how fuel and ammunition impact war – you can see the fuel gauge on your vehicle ticking down as you run out of gas, and you can calculate ammunition burn rates. You can see the cell phone battery drain but we lack the fundamental understanding or tracking of how much data is moving through the signals of our interconnectedness devices. Without gauges and a fundamental understanding of how much data is pushed (and pulled) from our devices, it is easy to forget or ignore the potential dangers of the free movement of data. We talk about storing data on the cloud – something fluffy and far away instead of calling it what it is: other people's computers. Putting data on someone else's computer implies a lot more risk than a cloud.

We tell commanders they must understand the operational environment but how do you train leaders to understand the types of data that are available on your unit when you don't know what questions to ask? This lack of understanding is not willful ignorance but rather a lack of literacy on both what data is, how it is generated from everyday activities such as buying medication or getting directions, and how we actually utilize data in daily and military life. It is less clear how quickly different types of data be used or exploited on the modern battlefield or arguably more importantly, prior to open conflict because its interpretation is viewed as available to the purveyors of the dark arts who can understand it and hopefully explain the impact of it. The data as ammunition analogy (re)educates leaders to examine data by potential risk and puts data management in the more familiar territory of risk management.

Physical geography influences our understanding of our equipment limitations and resupply capabilities and the mapping of both threat and advantage in the physical space is clearly understood. Situation reports and concepts of the operation both list strengths in supply and personnel and risk levels for the mission. Less clear is how to categorize and understand how different types of data influence conflict and competition. Large-scale discussions over

resource control around oil-rich areas are easier to visualize and understand than datasets residing on a server somewhere. It is precisely because of the unknown and unclassified vulnerabilities in the vast amounts of available data that a new framework is needed for conceptualizing the risk that data poses to manage that risk.

Rethinking and remapping the digital space as lines of supply/communication on the battlefield brings an awareness that there is a risk to the force if they are not secured in the same way we secure our physical lines of communication. Digital lines of communication are more porous and vulnerable, made further so by the easily accessible data carried on our personal devices. We go to great lengths to ensure ammunition is not easily accessible; how much riskier is it to ignore the easy access of personal data about our personnel? It is difficult to understand the vulnerability that the commercial and unregulated purchase of data poses when we think of it only as individual bits, but as any soldier who's had to police the wood line for a round of ammunition will tell you, the potential threat that one unaccounted for round poses is real. Those individual rounds of data do not pose threats in and of themselves, but the potential weaponization through analytics ought to grant us pause in the same way we would comb the wood line for a round of ammunition.

## UXO: UNEXPLODED ORDNANCE OR THE UNKNOWN POTENTIAL OF DATA

As shown in Figure 1, ammunition is typically classified by explosive type or family and moves from small arms for weapons such as an M4/AR15, through larger caliber weapons such as 125mm rounds to grenades, rockets through land mines, and larger explosives.[11] Important to this analogy, the different types of ammunition are typically used for different targets. Small arms rounds are used for smaller objects such as individual enemy soldiers whereas land mines, for example, are area obstacles meant to funnel personnel toward specific locations. Ammunition is further stored by hazard category and even smaller, less damaging rounds are segregated from other more combustible munitions. Similarly basic data, on its own, is not dangerous but when combined with analytics, can reveal powerful and potentially damaging insights.

**FSC Group 13 Classes**

| FSC Group 13 (classes) | Ammunition and Explosive Type or Family |
|---|---|
| 1305 | Ammunition, through 30mm |
| 1310 | Ammunition, over 30mm up to 75mm |
| 1315 | Ammunition 75mm through 125mm |
| 1320 | Ammunition, over 125mm |
| 1330 | Grenades |
| 1340 | Rockets and rocket ammunition |
| 1345 | Land mines |
| 1365 | Military chemical agents |
| 1370 | Pyrotechnics |
| 1375 | Demolition materials |
| 1376 | Bulk explosives |
| 1377 | Cartridge and propellant activated devices and components |
| 1390 | Fuzes and primers |
| 1395 | Miscellaneous ammunition |
| 1398 | Specialized ammunition handling and service equipment |
| 1410/20/25/27 | Guided missiles |

*Note: There are other FSC groups, but they are for Class V materiel outside the U.S. Army ammunition inventory. (Look in any current copy of the DOD ammunition listing, volumes 1 through 3, for more information.)*

Table 1. Table F-1, Appendix F (Department of the Army 2001a).

Data functions in a similar way to ammunition in the way that ammunition, when combined with a weapons system, creates different levels of destruction. Data is not inherently dangerous in and of itself and can be used for many different types of activities, some of which are objectively good, like using data to train machine learning algorithms to try to identify earlier means of identifying cancer. But thinking about data as ammunition can help conceptualize the potential risk it poses by tying that data back to the real people it represents rather than in an abstract form.

Consider microtargeting, a key piece of the information warfare battlefield[12] – which is the ability to develop a unique profile of an individual to ensure that advertisements are tailored to their specific interests.[13] Advertisers used to say that only 50% of advertising worked – they just did not know which 50%. Not all microtargeting is bad; arguably it can be used to help people find the things they are already looking for. Marketers know, for example, that it takes up to seven engagements with an advertisement before someone is moved to make a purchase. Microtargeting allows tailored advertisements to probe multiple times to get those seven engagements, including how often the target simply pauses over the ad. Microtargeting promises advertisers efficiency and effectiveness because it gathers significant amounts of data to promise accuracy. Microtargeted advertising is what enabled Meta/Facebook to dominate advertising for the last decade – the ability to push ads to people who may be interested in your product based on data that Meta/Facebook collected from users.[14]

Like ammunition storage units that house potential devastation wrought by one round igniting the others around it, a data storage unit contains the potential for devastating effects. Data in and of itself can be inert, but when massed (enriched) or honed for a specific purpose (analytics) it can wreak havoc and render targets ineffective by taking them out of the fight. There are hundreds of stories of data being used to target people at their most vulnerable. From gambling[15] to divorce[16] to addiction,[17] data can identify patterns or pattern changes in life that indicate opportunities for attack and exploitation. Collated data across these lived patterns further connects individuals to others, with the result of not only a precision round designed for the individual but also a cluster of these rounds that can damage or destroy important social relationships.

The same data that allows an advertising algorithm to help a shoe company find people in the market for shoes also allows a con artist to find people particularly vulnerable to scams and fraud or worse.[18] Amazon recently came under fire for its algorithm recommending a common food preservative along with other products that could be used for suicide.[19] Sodium nitrate is also widely used in food preservation– but the algorithm was not trained on data that enabled it to distinguish between someone looking for it for a legitimate purpose compared to one intended for self-harm. Just as we do not store dangerous products in the vicinity of each other, nor should we accept storing dangerous data in the same proverbial closet.

## MODERN MINEFIELDS

If we accept the analogy that data is ammunition, then the analogy for the surveillance economy – everything from apps to internet usage to location data - is a minefield. A minefield can both injure unwitting individuals who step into it and funnel people and forces to places advantageous to the opposing force when known. In marketing, funnels are used to scan for people who might be interested in a product and use a series of gates to draw them further into the sales funnel until they complete a purchase. Think of companies that use sale items to get people into the store. Once they are in the store, the stores are designed in specific ways to increase the likelihood of additional purchases.[20] Minefields in real life function in a similar way, funneling people towards or away from an objective. In marketing, data provides the targeting information used to identify potential targets. In physical minefields, mines can be indiscriminate—injuring or killing anyone who happens by—or they can wait until just the right time to detonate on a specific target as happened in the Grozny Stadium bombing in 2004 where a bomb was built into the stadium during construction.[21] Data can be gathered and analyzed using machine learning to determine the greatest vulnerabilities and, similar to a minefield, they can be used to broadly target, or they can be set to target a specific individual at a specific time.

Having a single tweet or video go viral can be similar to the effect of stepping on a mine – and not only a virtual mine but one with real-life consequences.[22] Even more data is collected and aggregated on seemingly harmless and innocuous everyday life making it difficult to see the potential dangers. But if Target knows that someone is buying newborn diapers, then that data, collated with other data such as proximity to a military base can now inform an adversarial party that there is a high likelihood of an infant in a servicemember's home.[23] The physical boundaries of a kinetic fight are no longer the only battlefield concerns in the information fight but now cross war-time boundaries as well. Children of politicians have become national news stories overnight because of their social media posts or because the content of their private data lives has been exposed to the world. Targeting someone's family to influence their actions is not a new tactic – the ease with which the surveillance economy enables this targeting now is what's changed.[24]

## DEEPLY BURIED DATA IEDS

One problem with the data as ammunition analogy is that unlike physical ammunition, which is degraded over time by the elements and the bounds of physics, data does not always suffer the same limitations. Data, in all its forms, is collected and stored at an increasing rate, and through the advances in algorithms and artificial intelligence, collated on a scale unimaginable even twenty years ago.[25] While much of that data gathering can be used for individual and collective good—reducing shopping times and finding causes of health concerns—it can also have devastating effects. Photographs are records and digital copies of photographs can spread around the world in an instant for essentially zero cost and be collected

and stored by companies building facial recognition algorithms with no legal recourse for the person associated with said face.[26] Data as ammunition can be loaded into the weapon at the time and place of an adversary's choosing – meaning something you may have long forgotten about may suddenly be brought to the forefront, efficiently (re)using ammunition specifically tailored for you.[27] Another limitation of the data as ammunition analogy is that most of the data that would need to be categorized along these lines is not owned or controlled by the government – it is collected and stored by commercial entities.[28] However, there is a tendency to ignore or downplay the risks from ubiquitous technical surveillance. Dismissing the problem because "they already have everything" is like dismissing the bleeding wound. We don't dismiss risk to force or risks to mission in any other context. This, however, makes the analogy more important – we cannot ignore the risks commercial data and analytics pose to the force simply because we dismiss it as marketing data or something else harmless. Thinking about all data collection – commercial or otherwise - as potentially adversarial would go a long way to expanding how people think about data and risks to the force.

Data, like ammunition, is generally not as useful on its own as when combined with analytics. To go back to the ADP 3-13, data is interpreted by the receiver. In this case, we argue that the meaning of data is created not only through its collection but also through analytics, or for what it can be used. Data is inherently biased beginning with the decision to collect what by whom and when. The meaning it takes on is created the moment it is transcribed or captured and further modified depending on what it is used for.[29] If data is the ammunition, who has access to the data and what analytics they can run are the weapon system. There has been reporting for more than a decade about the outrage generated when the public becomes aware of someone having access to data they were not supposed to. The scale and scope of the data should be measured by its potential and access to it should be controlled just like we control access to ammunition. In much the same way, we have procedures when there has been a breach of ammunition storage or when ammunition is improperly accounted for, but we do not have procedures for notification when commercial data is legally shared/transferred.[30] We tend to pay attention to people who have large legitimate stockpiles of ammunition, yet we don't blink at companies stockpiling data.

Likewise, we ignore the fine print in the terms and conditions of apps we use for personal activities and then feel exposed when we find out that the same data is available to a third party for a price. The U.S. government is precluded from peering into citizen's lives without probable cause and yet commercial entities can collect, aggregate, sell, and transfer deeply personal data without considering the consequences to individuals.[31] Why wouldn't America's adversaries be acquiring this data for use with their analytics?

## DIGITAL IEDS REQUIRE NEW KINDS OF FORCE PROTECTION

In Army doctrine, defense sets conditions for the offense. Currently, there is limited to no defense for servicemembers and other members of the total force from commercial data

collection. Around the world, data and analytics are being used to speed up targeting while not necessarily ensuring accuracy.[32] People have lost jobs, divorced, been doxed, and harassed because a piece of data hit at exactly the right moment for malicious actors to take advantage of the algorithms deciding a story was worth amplifying.[33] If these things are happening to civilians, why would we think that our nation's adversaries are not considering how to deploy these same tools during periods of heightened competition or conflict? Why wouldn't an adversary leverage the ability to rapidly employ data through analytics to target people in their homes? This capability has already been deployed against the Uighur population and people who have been critical of China abroad.[34] It is now possible to leverage rapid analytics to identify people's homes, families, and routines to target them individually at scale to reduce the ability of the military to muster forces.[35] This is the equivalent technological advancement of the machine gun in World War I, by increasing the ability to put rounds downrange. Leveraging digital ammunition in non-conflict spaces could be dramatically more effective in impacting readiness levels than waiting until forces are massed on a battlefield.[36] These "wounds" could render the targets just as combat ineffective as the loss of soldiers and equipment.

Using this theory, we argue that we do not have to start from scratch for policy recommendations. We argue that given the framework of data as ammunition, we can then start adapting existing privacy policies, compartmentalization procedures, and data use policies to clearly articulate who should have access to what data and for what purposes, including restricting access by commercial entities to collect on servicemembers where allowed by law. Current privacy policies should include requirements for commercial entities to notify individuals before the sale or sharing of their data with a third party, rather than a blanket statement in the terms and conditions. Buying in bulk of certain items, such as fertilizer, triggers commercial and governmental algorithms. A farmer has a right to access and need for bulk fertilizer; a similar adaptation could exist for acquiring data in bulk: demonstrated need to know. This is part of the same language we use for access to classified information: cleared to know it and need to know.

Understanding the impact of data is important for classifying that data. In April 2024, the White House expanded on Executive Order 13873 of May 15, 2019, and limited the sale of bulk personal data to countries of concern. This executive order defined sensitive data as "covered personal identifiers, geolocation, and related sensor data, biometric identifiers, human'omic data (meaning data that characterizes various elements of individual human biology), personal health data, personal financial data, or any combination thereof, as further defined in regulations issued by the Attorney General"[37] which is to be restricted from sale to certain countries of concern. While there is still more to be done, it is significant that the executive branch is recognizing that some of the data readily available to us companies may pose a serious risk to the U.S. in the wrong hands.[38] For decades, service members used their Social Security Number for nearly every aspect of their daily military lives – which also linked them to many aspects of their civilian lives such as credit reporting, medical information, and cell

phone numbers.[39] Understanding the legitimate risks of having one government identification number available to so many agencies caused the DOD to create a DOD ID number.[40] Using information to identify a person for more than one purpose is convenient, but it is also dangerous and opens us up to individual, or organizational, attacks. This is also why, though frustrating at times, creating unique passwords for different accounts does provide a level of protection and limit access should a breach of one account database occur. By thinking of data as ammunition, we argue that we can require both universal safety for bulk storage and practical safety for individual storage as risk mitigation.

Information warfare is a new form of contact and data is the technological advancement of this changing character of modern war—it can be purchased commercially off-the-shelf, weaponized, stored long-term, and reused in new combinations to exploit vulnerabilities both long before forces ever begin to mobilize and on the battlefield. It is efficient and can be highly effective because of the low cost, durability, and real-time customization it provides combatants. Unlike the machines of war that are the domain of state actors, data and associated analytics are available widely and have a low barrier to entry – everyday activity can inadvertently provide ammunition to adversarial actors, from pop up social media games to posting pictures of family members on significant dates. Further, even if people want to protect their data, there are limited opportunities for service members or anyone without means to hire an army of attorneys to meaningfully opt out of the surveillance economy minefield.[41] Data is already ammunition purchased in broad daylight and on the black market—by friend and foe alike.

Data is the next evolution in munitions.[42] Just as we develop Army leaders to understand how to employ specific weapons platforms and mass fires for effects, we need to start developing leaders who understand how data and analytics can be leveraged both for force protection as well as offensive actions. It is foolhardy to continue to talk about being data-centric without developing leaders who understand the risks data and analytics pose to the force. It can and is being weaponized against our forces. Our would-be adversaries are already in the market and the Army would be foolish to ignore the ways that data they cannot control can become powerful weapons systems to use against their own forces.

## DISCLAIMER

The views expressed in this work are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

## NOTES

1. Gregg Zoroya, "How the IED Changed the U.S. Military," (December 18, 2013). USA TODAY, https://www.usatoday.com/story/news/nation/2013/12/18/ied-10-years-blast-wounds-amputations/3803017/.
2. Jessica Dawson, "Who Controls the Code, Controls the System: Algorithmically Amplified Bullshit, Social Inequality, and the Ubiquitous Surveillance of Everyday Life," (September 2023) *Sociological Forum*, Vol. 38, No. S1, https://doi.org/10.1111/socf.12907.
3. Jessica Dawson, "Microtargeting as Information Warfare," *The Cyber Defense Review* (February 2021): https://doi.org/10.31235/osf.io/5wzuq, 63-80.
4. Jessica Dawson and Tarah Wheeler, "How to Tackle the Data Collection behind China's AI Ambitions," (April 29, 2022) *Brookings Institute* (Online), https://www.brookings.edu/techstream/how-to-tackle-the-data-collection-behind-chinas-ai-ambitions/.
5. "The World's Most Valuable Resource Is No Longer Oil, but Data," (May 6, 2017). *The Economist*, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.
6. U.S. Department of the Army, *Information*, ADP 3-13. (November 2023) Washington, D.C.: Department of the Army, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN39736-ADP_3-13-000-WEB-1.pdf, 1-1.
7. Jer Thorp, *Living in Data: A Citizen's Guide to a Better Information Future (May 4, 2021). New York: MCD; Mary F. E. Ebeling, Healthcare and Big Data: Digital Specters and Phantom Objects, 1st ed.*, (September 28, 2016). New York: Palgrave Macmillan; Mary F. E. Ebeling, *Afterlives of Data: Life and Debt Under Capitalist Surveillance, 1st ed.* (June 14, 2022). Oakland, California: University of California Press, https://bookshop.org/p/books/afterlives-of-data-life-and-debt-under-capitalist-surveillance-mary-f-e-ebeling/17505478.
8. Daniel J. Solove and Paul M. Schwartz, "ALI Data Privacy: Overview and Black Letter Text," (February 23, 2022). *68 UCLA Law Review*, accessed in SSRN, https://doi.org/10.2139/ssrn.3457563, 1252-1300.
9. U.S. Department of the Army, Supply Bulletin SB 708-21: Federal Supply Classification (May 2005). Battle Creek, MI: Defense Logistics Information Service, https://gsaxcess.gov/htm/userguides/DRMS_H2_FSC_Guide.pdf, 4-7.
10. Drew Austin, "The End of Infinite Data Storage Can Set You Free," (March 16, 2022). Wired, https://www.wired.com/story/cloud-computing-space-data-storage-habits/.
11. U.S. Department of the Army, *Ammunition Handbook: Tactics, Techniques, and Procedures for Munitions Handlers, FM 4-30.13 (FM 9-13)*, (2001). Washington, D.C.: Department of the Army.
12. Dawson, 2021; Christopher Wylie, *Mindf*ck: Cambridge Analytica and the Plot to Break America* (October 8, 2019). New York: Random House; Laurie Clarke, "How the Cambridge Analytica Scandal Unravelled," (October 15, 2020). The New Statesman, https://www.newstatesman.com/science-tech/social-media/2020/10/how-cambridge-analytica-scandal-unravelled.
13. Byron Tau, "How the Pentagon Learned to Use Targeted Ads to Find Its Targets—and Vladimir Putin," (February 27, 2024). *Wired*, https://www.wired.com/story/how-pentagon-learned-targeted-ads-to-find-targets-and-vladimir-putin/; Almog Simchon, Matthew Edwards, and Stephan Lewandowsky, "The Persuasive Effects of Political Microtargeting in the Age of Generative AI," (January 29, 2024). *PNAS Nexus Vol. 3, Issue 2*, https://doi.org/10.1093/pnasnexus/pgae035.; Gus Lubin, "The Incredible Story of How Target Exposed a Teen Girl's Pregnancy," (February 16, 2012). *Business Insider*, https://www.businessinsider.com/the-incredible-story-of-how-target-exposed-a-teen-girls-pregnancy-2012-2.; Kashmir Hill, "How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did," (February 16, 2012). *Forbes*, https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.
14. Paul Hitlin, Lee Rainie, and Kenneth Olmstead, "Facebook Algorithms and Personal Data," (January 16, 2019). *Pew Research Center: Internet, Science & Tech* (Report), https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/; Shoshana Zuboff, "Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization," (July-September 2022). *Organization Theory Vol. 3, Issue 3*, https://journals.sagepub.com/doi/epub/10.1177/26317877221129290; Francis Haugen, "Testimony of Frances Haugen to the January 6th Committee," (December 17, 2021). Transcript, U.S. House of Representatives Select Committee to Investigate the on January 6th Attack on the U.S. Capital, Washington, D.C., https://archive.org/details/january-6th-committee-witness-testimony-20211217-frances-haugen.
15. Wolfie Christl, "Digital Profiling in the Online Gambling Industry," (January 2022). *Institute for Critical Digital Culture*, https://crackedlabs.org/en/gambling-data.

## NOTES

16. Rob Mudge, "US Religious Data Platform Targets Vulnerable People," (September 27, 2020). Germany: Deutsche Welle, Dw.Com, https://www.dw.com/en/us-religious-data-platform-targets-mentally-ill-vulnerable-people/a-55062013; Kendra Barnett, "The Repeal of Roe v Wade Will Impact Our Privacy Landscape at Large, Experts Predict," (June 24, 2022). London: *The Drum*, https://www.thedrum.com/news/2022/06/24/the-repeal-roe-v-wade-will-impact-our-privacy-landscape-large-experts-predict.
17. Juliana Gruenwald Henderson, "Alcohol Addiction Treatment Firm Will Be Banned from Disclosing Health Data for Advertising to Settle FTC Charges That It Shared Data Without Consent," (April 11, 2024). U.S. Federal Trade Commission, Press Release, https://www.ftc.gov/news-events/news/press-releases/2024/04/alcohol-addiction-treatment-firm-will-be-banned-disclosing-health-data-advertising-settle-ftc.
18. Alistair Simmons and Justin Sherman, "Data Brokers, Elder Fraud, and Justice Department Investigations," (July 25, 2022). *The Lawfare Institute*, https://www.lawfaremedia.org/article/data-brokers-elder-fraud-and-justice-department-investigations.
19. Megan Twohey and Gabriel J. X. Dance, "Lawmakers Press Amazon on Sales of Chemical Used in Suicides," (February 4, 2022). *The New York Times*, Technology Section, https://www.nytimes.com/2022/02/04/technology/amazon-suicide-poison-preservative.html.
20. Romain Dillet, "Google and Mastercard Reportedly Partner to Track Offline Purchases," (August 31, 2018). *TechCrunch Online*, https://techcrunch.com/2018/08/31/google-and-mastercard-reportedly-partner-to-track-offline-purchases/; Minna Ruckenstein and Julia Granroth, "Algorithms, Advertising and the Intimacy of Surveillance," (February 11, 2019). *Journal of Cultural Economy Vol. 13, No. 1*, 12–24, https://doi.org/10.1080/17530350.2019.1574866.; Hirsh Chitkara, "How Lax Social Media Policies Help Fuel a Prescription Drug Boom," (July 6, 2022). Protocol, https://www.protocol.com/policy/meta-tiktok-prescription-drug-ads; Eduardo Schnadower Mustri, Idris Adjerid, and Alessandro Acquisti, "Behavioral Advertising and Consumer Welfare: An Empirical Investigation," (April 3, 2024). SSRN Scholarly Paper, Rochester, NY, https://doi.org/10.2139/ssrn.4398428.
21. "2004 Grozny Stadium Bombing," NGTC Group Training (blog), United Kingdom, accessed April 1, 2022, https://www.ngtc.co.uk/2004-grozny-stadium-bombing/.
22. Davis Winkie, "Pat Donahoe, Civilian, Wants a Word with the Army," (January 5, 2022). *Army Times*, https://www.armytimes.com/news/your-army/2023/01/05/pat-donahoe-civilian-wants-a-word-with-the-army/.
23. Lubin, 20212.; Jon Keegan and Joel Eastwood, "From 'Heavy Purchasers' of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You," (June 8. 2023). The Markup," *The Markup*, https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you.; Anya E. R. Prince, "I Tried to Keep My Pregnancy Secret," (October 10, 2022). *The Atlantic*, https://www.theatlantic.com/ideas/archive/2022/10/can-you-hide-your-pregnancy-era-big-data/671692/.
24. Yohannes Lowe, Kevin Rawlinson, and Warren Murray, "Wife of Ukrainian Military's Top Intelligence Official Poisoned; Stoltenberg Urges Nato to 'Stay the Course' – as It Happened," The Guardian, November 28, 2023, sec. World news, https://www.theguardian.com/world/live/2023/nov/28/russia-ukraine-war-live-enemy-attempts-to-storm-avdiivka-from-all-directions-says-ukrainian-official.
25. Justin Brookman, "Understanding the Scope of Data Collection by Major Technology Platforms," (May 2020). *Consumer Reports*, https://innovation.consumerreports.org/wp-content/uploads/2023/05/Understanding-the-Scope-of-Data-Collection-by-Major-Platforms_2020_FINAL.pdf
26. Kashmir Hill, "A Face Search Engine Anyone Can Use Is Alarmingly Accurate," (May 26, 2022). *The New York Times*, Technology Section, https://www.nytimes.com/2022/05/26/technology/pimeyes-facial-recognition-search.html.
27. Kashmir Hill, "A Vast Web of Vengeance," (January 30, 2021). *The New York Times*, Technology Section, https://www.nytimes.com/2021/01/30/technology/change-my-google-results.html.
28. Ronan Farrow, "How Democracies Spy on Their Citizens," (April 18, 2022). *The New Yorker*, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens.; Finn Myrstad and Ingvar Tjostheim, "Time to Ban Surveillance-Based Advertising: The Case Against Commercial Surveillance Online," (June 22, 2021). Oslo, Norway: Forbruker Rådet, https://www.forbrukerradet.no/wp-content/uploads/2021/06/20210622-final-report-time-to-ban-surveillance-based-advertising.pdf.; Byron Tau, Andrew Mollica, Patience Haggin, and Dustin Volz, "How Ads on Your Phone Can Aid Government Surveillance," (October 13, 2023). *The Wall Street Journal*, https://www.wsj.com/tech/cybersecurity/how-ads-on-your-phone-can-aid-government-surveillance-943bde04.; Dell Cameron, "The US Is Openly Stockpiling Dirt on All Its Citizens," (June 12, 2023). *Wired*, https://www.wired.com/story/odni-commercially-available-information-report/.

## NOTES

29. Ebeling, *Afterlives of Data: Life and Debt Under Capitalist Surveillance.*
30. Hill, "A Face Search Engine Anyone Can Use Is Alarmingly Accurate."
31. Tau "How the Pentagon Learned to Use Targeted Ads to Find Its Targets—and Vladimir Putin;" Byron Tau, *Means of Control: How the Hidden Alliance of Tech and Government Is Creating a New American Surveillance State*, (February 27, 2024). New York: Crown; Hill, "A Face Search Engine Anyone Can Use Is Alarmingly Accurate;" Kashmir Hill and Corey Kilgannon, "Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies," (December 22, 2022). *The New York Times*, New York Section, https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html.
32. Melissa Heikkila, "Dutch Scandal Serves as a Warning for Europe over Risks of Using Algorithms," (March 30, 2022). *POLITICO, Europe Edition*: https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/.
33. Kelly Kennedy, "Short Changed: No Justice at Fort Hood for Another Woman Soldier and a Commander Who Tried to Help," (December 14, 2023). *The War Horse* (blog), https://thewarhorse.org/fort-hood-commander-punished-after-reporting-sexual-harasser/.
34. Elias Groll, "Chinese Hackers Target Family Members to Surveil Hard Targets," (March 26, 2024). *CyberScoop Online*, https://cyberscoop.com/china-hacking-family-members/; National Counterintelligence and Security Center, *China's Collection of Genomic and Other Healthcare Data from America: Risks to Privacy and U.S. Economic and National Security*, (February 2021). Washington, D.C.: National Counterintelligence and Security Center, https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact _Sheet_2021revision20210203.pdf.; Albert Zhang and Danielle Cave, "Smart Asian Women Are the New Targets of CCP Global Online Repression," (June 3, 2022). *The Strategist*, Australian Strategic Policy Institute, https://www.aspistrategist.org.au/smart-asian-women-are-the-new-targets-of-ccp-global-online-repression/.
35. Madhumita Murgia and Max Harlow, "Who's Using Your Face? The Ugly Truth about Facial Recognition," (September 18, 2019). United Kingdom: *Financial Times*, https://www.ft.com/content/cf19b956-60a2-11e9-b285-3acd5d43599e; Paul Lewis, "'I Was Shocked It Was So Easy': Meet the Professor Who Says Facial Recognition Can Tell If You're Gay," (July 7, 2018). *The Guardian*, https://www.theguardian.com/technology/2018/jul/07/artificial-intelligence-can-tell-your-sexuality-politics-surveillance-paul-lewis.; Ryan Mac, Caroline Haskins, and Logan McDonald, "Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA," (February 28, 2020). BuzzFeed News, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement; Hill, "A Face Search Engine Anyone Can Use Is Alarmingly Accurate;" Hill and Kilgannon, "Madison Square Garden Uses Facial Recognition to Ban Its Owner's Enemies."
36. Tim Kane. *Bleeding Talent: How the US Military Mismanages Great Leaders and Why It's Time for a Revolution*. (January 4, 2013). New York: Palgrave Macmillan; Gareth Corfield, "Why LinkedIn Is a Snooper's Paradise," (August 24, 2023). *The Telegraph*, https://www.telegraph.co.uk/business/2023/08/24/how-linkedin-became-a-hotbed-for-spying/.
37. President Joseph R. Biden Jr., Executive Order 13873, *Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*, (February 28, 2024). The White House, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/02/28/executive-order-on-preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data-by-countries-of-concern/.
38. Dan Lamothe, "China's Military Seeks to Exploit U.S. Troops, Veterans, General Warns," (September 9, 2023). *The Washington Post*, https://www.washingtonpost.com/national-security/2023/09/08/china-military-exploit-us-troops-veterans/.
39. Jim Routh, "The Emergence and Implications of Unconventional Security Controls," (July 1, 2017). *The Cyber Defense Review Vol. 2, No. 2*, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Emergence%20and%20Implications%20of%20Unconvential%20Security%20Controls_Routh.pdf?ver=2018-07-31-093712-843, 35–44.
40. U.S. Army Training and Doctrine Command, "Information Paper: Department of Defense Identification Number," (October 2020). https://www.tradoc.army.mil/wp-content/uploads/2020/10/DoD-ID-Number-PII-Policy-2.pdf.

## NOTES

41. Steven Melendez and Alex Pasternack, "Here Are the Data Brokers Quietly Buying and Selling Your Personal Information," (March 2, 2019). *Fast Company*, https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information.; Kashmir Hill, "General Motors Quits Sharing Driving Behavior with Data Brokers," (March 22, 2024). *The New York Times*, Technology Section, https://www.nytimes.com/2024/03/22/technology/gm-onstar-driver-data.html; Justin Sherman, Hayley Barton, Aden Klein, Brady Kruse, and Anushka Srinivasan, "Data Brokers and the Sale of Data on U.S. Military Personnel," (November 2023), Duke University, Sanford School of Public Policy, https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf.; Henrik Twetman and Gundars Bergmanis-Korats, "Data Brokers and Security," (January 14, 2021). NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/publications/data-brokers-and-security/17; Ari B. Friedman, Raina M. Merchant, Amey Maley, Karim Farhat, Kristen Smith, Jackson Felkins, Rachel E. Gonzales, Lujo Bauer, and Matthew S. McCoy, "Widespread Third-Party Tracking On Hospital Websites Poses Privacy Risks For Patients And Legal Liability For Hospitals," (April 2023). *Health Affairs Vol. 42, No. 4,* 508–15, https://doi.org/10.1377/hlthaff.2022.01205; Gennie Gebhart and Josh Richman, "Science Shouldn't Give Data Brokers Cover for Stealing Your Privacy," (June 12, 2023). *Scientific American*, https://www.scientificamerican.com/article/science-shouldnt-give-data-brokers-cover-for-stealing-your-privacy/; U.S. House of Representatives Committee on Energy and Commerce, "Letter to Mr. Chat Engelgau, CEO Acxiom LLC," (May 10, 2023), https://d1dth6e84htgma.cloudfront.net/05_10_2023_Acxiom_Data_Brokers_Letter_1cbb81da32.pdf?updated_at=2023-05-10T16:19:56.031Z.; Lauren Feiner, "Lawmakers Press Companies That Collect U.S. Consumer Data to Reveal How They Buy and Sell It," (May 10, 2023). CNBC, https://www.cnbc.com/2023/05/10/lawmakers-press-data-brokers-to-reveal-how-they-buy-sell-information.html.
42. Kehrt, Sonner, "Troops, Veterans Are Targets in the Disinformation War, Even If They Don't Know It Yet." (September 1, 2022). *The War Horse* (blog), https://thewarhorse.org/military-veterans-learn-to-fight-disinformation-campaigns/.