REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
30 May 2018	Final	

4. TITLE AND SUBTITLE

The Algorithm of You: Your Profile of Preference or an Agent for Evil?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Dr. James J. Peltz

Paper Advisors: Dr. Yvonne Masakowski and Dr. Timothy Schultz

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Ethics and Emerging Military
Technology Graduate Certificate
Program
Naval War College
686 Cushing Road, Newport, RI

8. PERFORMING ORGANIZATION REPORT

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.
Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the EEMT Graduate Certificate Program. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC, the Department of the Navy, or the Department of Energy.

14. ABSTRACT

This essay explores the topic of individual user's data collected from mobile applications (apps) in the context of the ethical and legal implications that stem from informed consent given to the app developers through privacy and terms of use agreements. Of particular interest are the threats posed to the U.S. military as well as the ethical dilemmas posed by these activities to the populace writ large. After all military personnel are also private citizens and these data collections are particularly troubling since they enable effective profiling and allow adversaries to do the same. The ubiquitous nature of the digital world allows a robust model of a particular user to be built from the voluminous records that track and record their behaviors. This too has implications on national security as algorithms could ultimately be employed as surrogates for individual people.

15. SUBJECT TERMS

Data collection, privacy, ethics in emerging technology, machine learning

16. SECURITY CLASSIFICATION OF: Unclassified			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Thomas Creely
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		36	19b. TELEPHONE NUMBER *(include area code)* 401-841-7542

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE

Newport, R.I.

The Algorithm of You: Your Profile of Preference or an Agent for Evil?

By:

Dr. James J. Peltz

Department of Energy, National Nuclear Security Administration Civilian

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Ethics in Emerging Military Technology Graduate Certificate Program.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of Energy.

30 May 2017

UNCLASSIFIED

Acknowledgements

I wish to thank my advisors, Professor Yvonne Masakowski and Dean Timothy Schultz, for their thoughtful guidance during the performance of this work. I wish also to thank Mrs. Isabel Lopes for her many stimulating discussions and library assistance, as well as, Mr. Michael Ricker for his assistance in collecting and reviewing countless terms of service agreements.

Contents

Introduction

The digital world, enabled by fleets of sensors which include your mobile device, collects and stores information on the environment and you. Collect enough benign information about your buying habits, how and with whom you communicate, and the frequency with which you do it, and a digital shadow of you emerges with your unique characteristics, interests, values, beliefs, and social network. If you have ever used a service to analyze your DNA, then you've given a means to link this behavioral information with your unique physical identifier. Think of all the ways in which these data are used for better marketing of the products that you need. Now think of how you can be hacked, tracked, monitored, and recorded. These are challenging times for those who want to maintain a sense of privacy.

All of these data are collected legitimately because you agree to it. Every time you download an app for your phone or use a free service provided on the internet you are prompted to review a terms of service agreement. But how often do you read it? Do you know how companies use your data? Do you know that some of these agreements give permission for them to collect information about your friends, relatives, and even your children? "[P]ersonal data collected from children may include students' names, email addresses, grades, test scores, disability status and health records, suspension and discipline data, country of birth, family background, and […] may even include internet search history, videos watched, survey questions, lunch items purchased, heart rate and other biometric information measured during gym class, and even classroom behavior, such as being off-task or speaking out of turn."[1] Do you also know that the

[1]Valerie Strauss, "Personal Data Is Collected on Kids at School All the Time. Here's Help for Parents to Protect Children's Privacy," *The Washington Post*, May 16, 2017, https://www.washingtonpost.com/news/answer-sheet/wp/2017/05/16/personal-data-is-collected-on-kids-at-school-all-the-time-heres-help-for-parents-to-protect-childrens-privacy.

current paradigm leaves little Fourth Amendment protection of privacy from unlawful government seizure?[2]

How can they do this you might ask. They—commercial companies, the government and other third parties—do it by making the terms of service too long, too complex, and too confusing. In the U.S. they do it by lobbying Congress and ensuring that default options for using any of these apps are set to maximum share. Anytime you want more privacy, it's your job to find the settings and adjust them accordingly. Conveniently for them, there is no option to use a free service and have none of your data collected. The U.S. Judiciary also adds to the confusion from understanding the technology in different ways and confounding the doctrine used to evaluate privacy protections.[3]

Is this collection worth the risk to your privacy? Is it just creepy and evil, or is it unethical? You'll have to decide this for yourself. However, this paper reviews some of the critical issues. It also offers recommendations for changing the current paradigm of maximum sharing and collection by evaluating privacy from the three grand traditions of ethics: virtue theory, deontology, and utilitarianism. After all you, your friends, and your neighbors occupy all levels of local, state, and federal government, as well as the military that can be targeted, surveilled, and/or abducted at any time. Therefore, a discussion of some potential threats to both individual users and the state is also included.

[2] U.S. Const. Amend. IV.: The right of the people to be secure in their persons, houses papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things being seized.

[3] Monu Bedi, "The Fourth Amendment Disclosure Doctrines," *The William and Mary Bill of Rights Journal 2*6, no. 2 (2017): 494, Retrieved from https://search-proquest-com.usnwc.idm.oclc.org/docview/2023675687?accountid=322.

2

How Do Machine Learning and Data Collection Work?

Machine learning in the generic sense is algorithmic methods that identify, understand, and predict patterns in data; in other words, the algorithm is a relation map between inputs and outputs.[4] "Machines learn by studying data to detect patterns or by applying known rules to: categorize or catalog like people or things, predict likely outcomes or actions based on identified patterns, identify hitherto unknown patterns and relationships, and detect anomalous or unexpected behaviors."[5] The concept underpinning machine learning is to give the algorithm a massive number of "experiences" (training data) and a generalized strategy for learning, then let it identify patterns, associations, and insights from the data. In short, these systems are trained rather than programmed.[6]

Machine learning algorithms: supervised, unsupervised, semi-supervised, and reinforced are categorized by the way in which they are trained. Kimberly Nevala provides a primer covering the general uses, applications, and data requirements but for convenience, the following definitions are provided:

> **Supervised learning** provides the algorithm with well characterized (i.e., labeled) inputs and outputs to determine correlations and logic that can be used to predict an answer. **Semi-supervised learning** is similar in that a set of data are labeled but the algorithm is also provided unlabeled data in order to let the algorithm extrapolate identified correlations and logic from one to the other. **Unsupervised learning** allows the algorithm to parse the training data for correlations and relationships, much in the same way humans observe the world. In **reinforcement learning**, actions, rules, and potential end states are defined a priori, and then the algorithm learns to exploit the rules to create an optimal desired outcome.[7]

---

[4] Kimberly Nevala, *The Machine Learning Primer* (Cary, NC: SAS Institute, 2017), 5, https://s3.amazonaws.com/baypath/files/resources/machine-learning-primer-108796.pdf

[5] Nevala, *The Machine Learning Primer*, 5.

[6] Nicolaus Henke, et. al., *The Age of Analytics: Competing in a Data-Driven World*, McKinsey Global Institute Report, 2016, 11, https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world.

[7] Nevala, *The Machine Learning Primer*, 14-18.

A great deal of knowledge and work goes into understanding these methods, the voluminous data needed to support the various methods, and the acquisition pipelines to get these data i.e., "[The] governance policies and the data ecosystem must support exploratory environments (often referred to as sandboxes) as well as production environments."[8] Validation is another key task which involves making sure the right answer in these mappings is obtained for the right reasons which can be quite time-consuming and resource intensive in its own right.[9] The need for data and the need to understand if the right answers are obtained for the right reasons are large drivers for those collecting and analyzing these data.

Data Characteristics and the Collection Ecosystem

Everything in the world today revolves around making the most of data or making data work optimally for an intended user. Apps and the internet—portals to the digital world, increasingly link people, make it easier to share ideas, easier to make reliable predictions, and can even foster and enable civil unrest. Humans generate and consume data in the more familiar forms of blogs, emails, pictures, videos, and many other formats. They also generate data in the form of measurements and observations of the natural world in a variety of raw forms capturing weather data, observations of deep space, and those of fundamental particles of the universe. As summarized from McKinsey Global Institute,

> Some of the broad categories include behavioral data (capturing actions in both digital and physical environments), transactional data (records of business dealings), ambient or environmental data (conditions in the physical world monitored and captured by sensors), geospatial data, reference material or knowledge (news stories, textbooks, reference works, literature, and the like), and public records. Some data are structured (that it, easily [is] expressed in rows and

[8] Nevala, *The Machine Learning Primer*, 50.

[9] James Joseph Peltz, "Demonstrating Predictive Confidence for a Paradigm Dissolver Model using Methods for Evaluating Higher Order Moments: A "Case Study" for Nuclear Nonproliferation," (PhD diss., Karlsruhe Institute of Technology, 2016, 19, http://primo.bibliothek.kit.edu/primo_library/libweb/action/search.do.

> columns), while images, audio, and video are unstructured. Data can also come from the web, social media, industrial sensors, payment systems, cameras, wearable devices, and human entry. Billions of mobile phones, in particular, are capturing images, video, and location data. On the demand side, data can provide insights for diverse uses, some of which are more valuable than others.[10]

These data are all used to make predictions about human populations and trends about those populations.

Users who search, stream, and share pictures and videos via the internet or by the use of apps represent a market that can be bought and sold because although they are consumers of these products, they are also producers.[11] Thus, "advertisements on the Internet are frequently personalized; this is made possible by surveilling, storing, and assessing user activities with the help of computers and databases. In the case of the Internet, the commodification of audience participation is easier to achieve than with other mass media."[12] The direct apps and their developers are the first of many beneficiaries of such data. Recorded Future, a private data analytics company started in 2009, claims to make use of machine learning and natural language processing (NLP) to continuously analyze threat data from a massive range of sources thus predicting them before they happen. [13] And of course, the Arab Spring was facilitated by social media apps and global connectivity.[14]

---

[10] Nicolaus Henke, et. al., *The Age of Analytics: Competing in a Data-Driven World*, McKinsey Global Institute Report, 2016, 6, https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world.

[11] Valencia Rincon and Juan Carlos, "Internet and Surveillance. The Challenges of Web 2.0 and Social Media," *Revista Signoy Pensamiento*, Vol. 31, Núm. 61 (2012): 55-56.

[12] Rincon, *Revista Signoy Pensamiento*, 55-56.

[13] Recorded Future, "Threat Intelligence Machine," http://www.recordedfuture.com/technology/. Accessed on March 31, 2018.

[14] Jessi Hempel, "Social Media Made the Arab Spring but Couldn't Save It," *WIRED*, January 26, 2016, https://www.wired.com/2016/01/social-media-made-the-arab-spring-but-couldnt-save-it/.

Value to these data often depends on the structure and the contextual information about how, when, and who generated them. Access to analyze them is another critical factor. As the McKinsey report goes on to describe,

> [V]aluing data is difficult because of the diversity of these data. Relevant statistics for several areas that relate to users' privacy exist such as location-based services, healthcare, and retail markets are included to provide some context of monetary scale estimated to be in the 100s of billions. Estimates for GPS navigation devices and services, mobile phone location, and geo-targeted mobile advertising are on the order of $100B annually while another $700B is estimated in value provided to users from these services. Retail services benefit from the transaction based and behavioral data from their customers which is abundant and could be used to increase net margins by up to 60 percent. These numbers are reported to be similar for EU markets as well. Data analytics is estimated to be able to tap into the $300B value for U.S. healthcare which is potentially enabled by the rapid expansion of digitized medical records, now estimated to be 3 out of 4 patients.[15]

While rapid advances continue, barriers to tapping into the value of these areas are strict regulations evidenced by those which govern healthcare. It is not that surprising then to see why the current paradigm of opting out regarding data collection exists as discussed in the subsequent sections.

In terms of volume, a commercial data management company, Domo, updates a graphical depiction of the volume of data produced each minute of every day. Their fifth version of Data Never Sleeps graphic. Figure 1, released in 2017 details the rate at which data is created and consumed via the internet. In the span of just seven years, the global internet community increased from 400 million in 2000, to 3.2 billion in 2017.[16] Over half of these data come from mobile devices and are projected to increase to seventy-five percent of this volume in 2018. [17] This represents significant potential in terms of understanding the people generating these data,

[15] Nicolaus Henke, et. al., *The Age of Analytics: Competing in a Data-Driven World*, McKinsey Global Institute Report, 2016, 30-33, https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world.

[16] Josh James, "Data Never Sleeps 5.0," *Domo Blog*, Last modified July 25, 2017, http://bit.ly/2uvd4nH.

[17] James, *Domo Blog*.

and companies such as Domo are collecting them in the hopes of using data to generate money in the form of sales and marketing and consumable products.

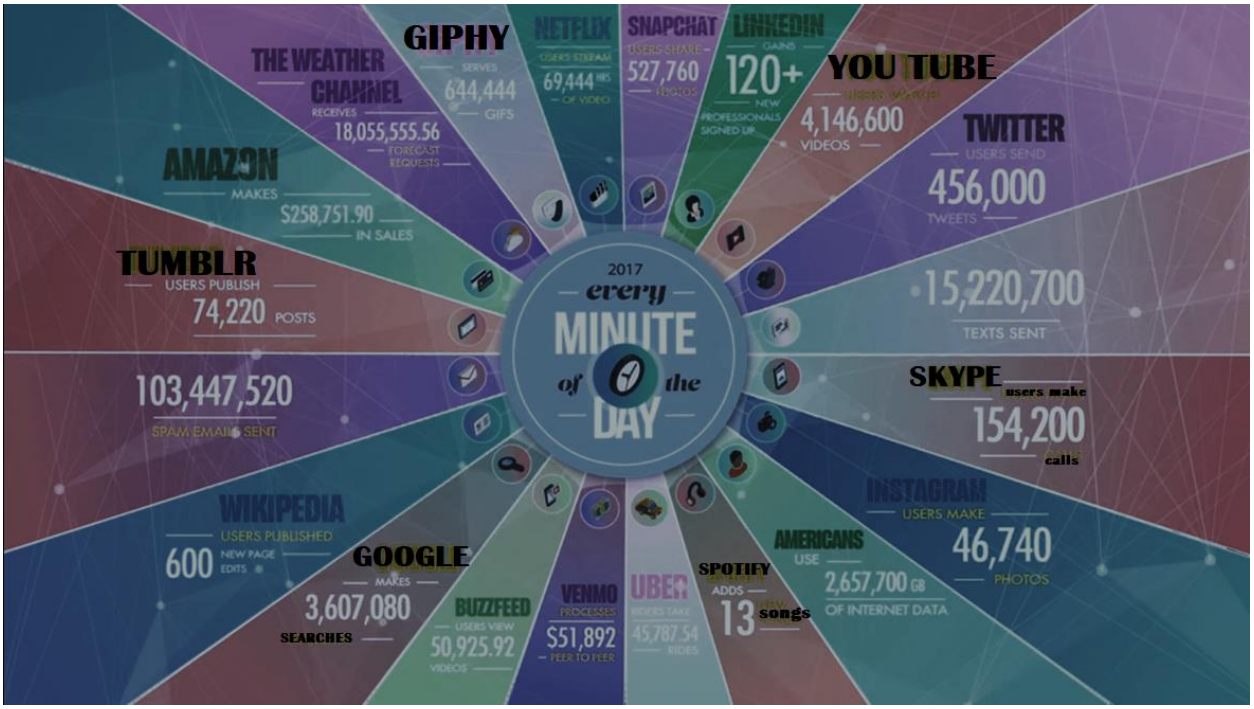

Figure 1. from https://www.domo.com/blog/data-never-sleeps-5/ showing the amount of data generated and consumed per minute on the internet.

As Domo advertises, "Data never sleeps, but Domo has compiled the latest statistics [so you or your business] can discover newer and faster ways to turn data into ah-hahs, to turn ah-hahs into to-dos, and to turn to-dos into cha-chings."[18] The cha-chings in this context are the dollars and revenue that come from the data service provider making it easier for the consumer or data generator to get the most use out of their own data. This concept plays out in numerous variations where the data generated by consumers is used by data analyzers to make these data "work" better for the consumer. Companies such as McKinsey and Domo are quite representative of the third parties that seek and harvest user data. However, what users may not appreciate is that the U.S. Government is able to *bypass* the Fourth Amendment protections

[18] James, *Domo Blog*.

under the third party and public disclosure doctrines which apply to websites and apps.[19] One recent example is the apprehension of the Golden State Serial Killer—A man who terrified California residents starting the in the late 1970s was apprehended by using a genealogy database.[20]

It's easier than ever to send off for a report on one's DNA. As a unique identifier, DNA also contains information about one's ancestry and predisposition for health, and while the current ability to identify individuals based on DNA is difficult, the number of people voluntarily pursuing this is increasing as the task becomes easier.[21] Investigators first used a genealogy website to identify a New Hampshire suspect, a man who eventually was convicted of multiple rapes. Investigators working on the Golden State Serial Killer case learned of these same techniques and decided to create a fake profile on a genealogy website and then uploaded genetic data to identify relatives of the suspect.[22] That suspect as of 5/15/18 is currently awaiting trial. These same websites also present would be customers with questionnaires about lifestyle and preferences. It is not a great leap nor that difficult to imagine the link that this information could provide insurance companies or healthcare providers.

Data Collection and the Current Paradigm of Privacy

The current paradigm of data collection and privacy in the U.S. could not be more in contrast with the idea of informed consent. The burden is on users to opt-out of agreements rather than the opposite, to opt-in to sharing their data. The realm of data collection in the free capitalist

[19] Cullen Hoback, *Terms and Conditions May Apply*, Documentary Film, 2013, Slamdance Film Festival, Park City, Utah, USA, 2013.

[20] Tim Arango, "The Cold Case That Inspired the 'Golden State Killer' Detective to Try Genealogy," *The New York Times.* May 3, 2018, https://www.nytimes.com/2018/05/03/us/golden-state-killer-genealogy.html..

[21] Maggie Fox, "What You're Giving Away with those Home DNA Tests," *NBC Health News*, updated Nov 30, 2017, https://www.nbcnews.com/health/health-news/what-you-re-giving-away-those-home-dna-tests-n824776.

[22] Arango, *The New York Times*, May 3, 2018.

markets is heavily influenced by commercial and advertising interests who advocate for fewer restrictions. The rapid pace of development tends to outpace laws and regulations that govern them and the full consequences fail to appear until much later. As recent events regarding Facebook and Cambridge Analytica show, it is not a problem until it's revealed as a problem.

The data Cambridge Analytica reportedly gathered in early 2014 through an app called "thisisyourdigitallife" was used to sway elections for the U.S. 2016 Presidential election where apparently 30 million "psychographic" profiles were created in order to send targeted political ads. The company is also linked to pro-Brexit campaign groups and data firm AggregateIQ for digital marketing services where it is reported Vote Leave's efforts were responsible for the victorious outcome to leave the European Union (EU).[23] Mark Zuckerberg, CEO of Facebook repeatedly speaks of privacy in the context of users controlling what they share, but this has little to do with what data are collected. After all, his objective isn't focused on an individual's privacy or security but rather to ensure profits for his stockholders.

The testimony to Congress by Zuckerberg in April of 2018 revealed the general ignorance and lack of concern around issues of individual privacy and how collected data are shared by a variety of stakeholders.[24] The current construct uses "consent," usually a checkbox from the user to get access, collect, and share data from the user through the terms-of-use and privacy agreements. What users often fail to consider is that these agreements grant permissions to a whole host of collectors and harvesters of their data in ways the user may not understand or in ways that take years or decades to experience. Similar to the complexity of bank mortgage

[23] Al Jazeera News, "Cambridge Analytica and Facebook: The Scandal So Far," News Privacy & Surveillance, March 28, 2018, https://www.aljazeera.com/news/2018/03/cambridge-analytica-facebook-scandal-180327172353667.html.

[24] The New York Times, "Mark Zuckerberg Testimony: Senators Question Facebook's Commitment to Privacy," Politics, April 10, 2018, https://www.nytimes.com/2018/04/10/us/politics/mark-zuckerberg-testimony.html.

documents, the language of these agreements is vague and filled with legal jargon often crafted to protect the interest of the bank or private industry, rather than to protect the rights of the user.

Economics of Privacy

What about the economics of privacy? "At its core, the economics of privacy concerns the trade-offs associated with the balancing of public and private spheres between individuals, organizations, and governments."[25] Alessandro Acquisti, Curtis Taylor, and Liad Wagman (2016) provide a thorough treatment of the definition of privacy and discuss tradeoffs associated with privacy and sharing of personal data. Three major themes are discussed:

1) understanding the context of privacy and economic relevance;
2) a discussion of scenarios between the individual and society where protection of privacy can both enhance and detract welfare; and
3) how informed decisions regarding privacy depend on a n understanding of how these data will be used.[26]

These categories more or less line up with the themes that are present in the vignette that follows and the categorical ethical discussions within each of the grand traditions to be discussed next. Notably, societal values change over time and are heavily influenced by the understanding of those examining the issue.

As evidenced by the commercial marketplace, the money behind these activities is substantial and there would be significant costs in changing the current business model for collecting these data. The question remains, what about the risks? For example, we can imagine the level of harm done as a result of the recent breach of personal data from security clearance forms at the DoD Office of Personnel Management. It is not too difficult to imagine a scenario

[25] Alessandro Acquisti, Curtis Taylor, and Liad Wagman, "The Economics of Privacy," *Journal of Economic Literature* 54, no. 2 (2016):443.
[26] Acquisti, *Journal of Economic Literature,* 443, 449.

where adversaries can threaten a country's national security with direct access to sensitive personnel records to people of the military.

Ethics of Privacy: *A Day in the Life of the Average Digital Citizen*

The following vignette provides a narrative to describe the convenience that is enabled by the sharing of data. It is intended to story-board a scenario argued by advertising and commercial advocates while also being used to illustrate the fine line that exists between convenience and that of being bound. A discussion of privacy then follows using the three ethical grand traditions to see what these schools of thought can convey on the matter.

Scene: EXT. ANYTOWN, USA: MORNING-SUNRISE

It's 7:00 a.m. as indicated by your phone's alarm. Instantly, notifications appear with events, news, and notifications of the events that happened while sleeping or for the upcoming day. The sleep app reports another restless night, not enough REM phase hours and two interruptions for the bathroom. Coffee is already brewing, courtesy of the routine morning app that sequentially adjusts the temperature, lights, and has the TV reporting the morning news. It's your mom's birthday and a confirmation for the roses that were suggested two days ago appear on a text balloon on the phone with a projected afternoon delivery. All of this information is seamlessly integrated courtesy of the synced location services (SLC) with the phone which is cross-linked to both your credit and bank accounts for additional security.

It is a run day as proclaimed by the fitness app, and the snapshot of your progress over the last two months shows a stagnating fitness level and a flag of concern regarding the last two days of evening meals that were deviations from the prescribed plan. The weather this morning is 55 degrees Fahrenheit, partly cloudy and the sidewalks and trails are damp from the night fog. You

heed the warning balloon and wear all-weather shoes and an extra layer as it flashes across as a headline. The suggested route appears and will be monitored via GPS and by heart rate in sensors within the shoes and the smart material in the jogging apparel. Map features from another app are integrated with the heart monitors to ensure the safest and optimal path for fat-burning which will be adjusted in real time based on topography and corresponding heart rate.

Upon returning from the run, the smart home's voice goes over the days to do list and then covers the household goods that are queued for order. The list is generated from the appliances that are connected via the Internet of Things (IoT) technology. The algorithm is even robust enough to make correlations about the health and mood of the user based on buying habits, voice inflections, and patterns of behavior of the users who use the device. Today, the car service was requested early since the roads were slick and the morning run was terminated early. In transit, the routine logic game is played which claims to measure a variety of parameters related to IQ and emotional intelligence. Results are publicly released to other users of the app and your friends on Facebook to ensure broader participation.

Arriving at the office, the computer is at the ready queued up from a new energy saving program which monitors the location of the proximity cards used to enter the building. The virtual assistant provides descriptions of 400-calorie lunch options that are part of the fitness plan and queries whether invitations should be sent to the colleagues who regularly join and because it's one of their birthdays. This information is gathered from recent conversations overheard by lunchtime app and feeds from the various social media apps. The day is routine and consists of shuffling around from various meetings, while notes and memos are kept by the virtual personal assistant. The last appointment is indicated as a telecon that is set up for the car ride home. The evening is already planned too when your friends indicated they would arrive from San

Francisco that evening. Personal organizers requested access to both schedules and these virtual assistants will coordinate behind the scenes adjusting schedules according to any delays. A new Vegan restaurant is suggested as the meeting point due to its location, their dietary restrictions, and the strict fitness plan. It also received good ratings and strong reviews.

Isn't this world extremely convenient? The ease with which tasks are automated can result in significant savings in time, energy, pollution, and yield a number of positive outcomes. Allergies can be identified and correlated with the various products you buy and avoid. Targeted achievements such as fitness and heart rate can adapt in real time and could call for the authorities in cases perceived to be an accident. Even personal relationships can be better managed because being nice could be automatically programmed. The diversity of data when cross-linked such as multiple bank accounts and credit could even become added security because access to all of them would require changes to one. But what is the cost of this convenience? What are the ethical considerations for all involved?

Virtue Theorists—*Privacy is Personal*

Borrowing from Socratic thought, "virtues such as justice are founded upon some basic moral knowledge, a knowledge which was sufficient to ensure correct conduct."[27] In the story of Euthyphro we, Socrates and Euthyphro, discuss the difficulties with defining the term holy because of the circular logic that often prevails, "when competing conceptions place emphasis on the acceptance of religions, traditions, and precedent instead of relying on the individual's power to discriminate between right and wrong both in the belief and action."[28] Such is the case here with privacy, where the power to discriminate between right and wrong, relies on the knowledge

[27] Plato, *The Last Days of Socrates*, London Penguin Group, 2003, xxxii.
[28] Plato, *The Last Days of Socrates*, xxxii.

of the individual whose concepts of privacy and value vary based on numerous factors and experiences. *A common extensible definition is needed.*

What this story emphasizes, too, is that virtue ethics relies heavily on the individual to cultivate said virtues. That said, it's not clear how virtue ethics alone could best examine the issue since, "This is problematic in that performing research on the strength of privacy norms becomes an exercise in testing the presence of an analyst's conception of privacy in a given population, for a given stakeholder, for a given issue."[29] However, one could certainly make the premise that *trust is the core element of privacy and thus privacy agreements are agreements that define trust so should be crafted to preserve this intention*.

Reviewing the day in the apps story from this perspective makes one see that all of this automation is also self-reinforcing. It's convenient and easy to follow which makes one agree to whatever is embedded in the terms and conditions to use the service. As the number of people participating increases, then what used to be a choice now becomes a binary decision of whether to use or not use a service. Gifts and remembering anniversaries, birthdays, etc., becomes as automated as junk mail. This process is part of what establishes a socio-cultural norm of *accepting* to share rather than an individual *choosing* to share.

Deontologists—*to Share or not to Share?*

The intent-based principle, that of pure reason, and the "categorical imperative," for duty sake alone are the core values of duty ethics and the deontologist. Deontologists are particularly concerned about the duties that free and reasonable creatures (paradigmatically, human beings)

[29] Kirsten Martin, "Understanding Privacy Online: Development of a Social Contract Approach to Privacy," *Journal of Business Ethics* 137, no. 3 (Sep 2016, 2016): 562-563, https://search.proquest.com/docview/1811874287?accountid=322.

owe to one another, particularly with respect to choosing actions that do not violate each other's rights.[30] "Although lying or testifying to what one does not believe is true, is for Kant, at the heart of all vice because it corrupts the internal relation of the self to its own dignity, we are under no general obligation to reveal all that is true about ourselves or about others. (We are not even epistemologically well constituted to reveal 'all that is true' about ourselves or others since our access to anyone's [including our own] deepest intentions are fundamentally indirect."[31] This is what Sharon Anderson-Gold uses as the Kantian rationale for privacy which focuses not on an exact definition of, or right to, privacy but rather the concepts that indirectly encompass privacy.

This concept could easily be extended to this argument. What makes the current paradigm out of line is the default choice is automatically and, in some cases, unknowingly to fully share rather than a real conscious decision to share. Neither Google nor Facebook has a good reason for supporting when asked about defaults on openness rather than defaults set to full privacy. The only one who benefits from the former is the commercial interest collecting data on the individual.[32]

All of the apps being used in the vignette are routine and relatively benign but consider how much information is being collected, if all of these apps are defaulted to collect and share. The vignette shows they also collect social network information on relatives and associates. Children could easily be considered in this story and what rules exist to protect their right to privacy?

[30] James J. Giordano, *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns*, Boca Raton, Florida: CRC Press, 2015, 281.

[31] Sharon Anderson-Gold, "Privacy, Respect and the Virtues of Reticence in Kant," *Kantian Review* 15, no. 2 (2012): 40.

[32] Cullen Hoback, *Terms and Conditions May Apply*, Documentary Film, 2013, Slamdance Film Festival, Park City, Utah, USA, 2013.

Utilitarianism and the Greater Good: *A Counterintuitive View of Privacy*

Utilitarianism is concerned with choosing to act in ways that increase the greatest good for the greatest number. All things being equal, Tony Doyle lays out a logical case for why perfect voyeurism meets the definition for utilitarianism since "whether or not someone is preventing the agent from having knowledge is irrelevant as long as the victim is behaving just as she would have in a world in which she is not being observed."[33] He even goes on to say that happiness does increase since the general definition ignores how that happiness is derived. Also, that those looking to breach someone's privacy that comes from self-interest, out of curiosity, for kicks or profit, to discredit or blackmail will incur costs to achieve these goals so it's in [his] best interest to have [his] privacy protected.[34]

While the argument naturally focuses on the negative action of voyeurism rather than the concept of privacy, it would seem there are enough parallels between the invasion of privacy and that of "benign" data collection. In this case, it is apparent that the current paradigm supporting data sharing enjoys some merit with respect to a utilitarian view. That he goes on to assert when voyeurs are discovered they deserve the wrath of punishment because, "…accomplished voyeurs potentially do more harm and are harder to detect than dabblers, would-be effective snoops need a stronger disincentive than dilettantes to pursue their ''hobby.'' This means more severe sentences the longer the convict is found to have been engaged in the crime and the stealthier his methods."[35] It may be interesting to explore this latter line of reasoning, in other words, severely penalizing companies for infractions related to privacy, but it would require clear definitions and

[33] Tony Doyle, "Privacy and Perfect Voyeurism," *Ethics and Information Technology 11,* No. 3, (2009): 182, http://dx.doi.org.usnwc.idm.oclc.org/10.1007/s10676-009-9195-9 Retrieved from https://search-proquest-com.usnwc.idm.oclc.org/docview/222251629?accountid=322.

[34] Doyle, *Ethics and Information Technology,* 183.

[35] Doyle, *Ethics and Information Technology,* 187.

explicit evidence of any harm or damage. Otherwise, litigation would be drawn out, costly affairs and do little to change the current paradigm on data collection and privacy.

A Utilitarian view is also where the idea of privacy seems to be most challenged because the outcome dealing with threats to the many will always outweigh the privacy of the individual. The bottom line is that anytime an individual shares data with a third party via agreeing to terms of use agreements, they are in a sense waiving their rights to privacy because this technology is viewed as a public service through the eyes of the law.

The result is that tracking of an individual's third-party data such as DNA and location information is fair game for the government without the need for a warrant.[36] Monu Bedi provides a cogent discussion regarding third party and public disclosure doctrines, reviews current Supreme Court rulings, and puts forth, "[A] workable topology toward discussing whether and how these disclosure doctrines should, or should not, apply to future technologies," because, "[I]t is imperative [that] we understand the historical context and unique contours of each doctrine [because] they are not the same thing, nor has the Court applied them in the same way." [37] *The same topology is needed to understand the contours or boundaries between privacy as examined through the individual, society, and the existing consequences so that future threats can be addressed with ethical solutions.*

To this end, each grand tradition has advantages and shortcomings with respect to applying a universally accepted framework for how privacy should be handled. The next section will

[36] Bedi, *The William and Mary Bill of Rights Journal,* 494.
[37] Bedi, *The William and Mary Bill of Rights Journal,* 494.

provide some specific implications of such technology to the military to emphasize the importance of the findings from this section and the respective schools of thought.

Individual Convenience or Threat to National Security?

As the story suggests, apps on a phone are surprisingly adept at building an algorithm of the person using them. Most employ the use of location services, record contacts, collect and link who one communicates with, and what one consumes e.g., products, services, and data. All of this information describes the individual, their likes, and their networks. Income, education level, and numerous other attributes can be gleaned from these data and exploited to sell one products such as in the case with Amazon, Apple, or Google or to be used by con artists and government agents for more nefarious purposes.

With enough data about a system, or a specific target/person, predicting attributes or specific behaviors becomes possible. In the case of people, what items fill their needs leaves data for algorithms to be developed or data that algorithms can exploit. For example, algorithms can capture data about the average citizen's use of alarms, sleep monitors, workout logs, bank accounts, bills, grocery lists, and games. In addition, networks collect and use data of the individual using them as well as collecting data from others in their social network. A user's phone quickly becomes an accurate profiling agent. This is mainly because the user agrees to the collection and sharing of these data through those lengthy privacy agreements that are required to use the app in question.

"You are what you app" as they say, and it is becoming fairly easy to categorize and profile any number of individuals from the apps they use.[38] Social networking apps such as Snapchat,

[38] Jeanette Mulvey, "'Appitypes': You Are What You App, Study Finds," *TechNewsDaily,* February 16, 2011,

Instagram, and Twitter from Figure 1. are quite significant data generators. They link people and employ algorithms that over time create a profile of the individuals who use them. Who individuals chat with the most, whose content they like or dislike, and the frequency with which they communicate are all characteristics of that user. With the advent of hashtags, conversation topics become linked and searchable to a larger population of users as well as become prime examples of how social data become bridges to the physical places, things, and ideas. The more one participates in discussions or generating data for others to consume, the more extensive and detailed the algorithms in these apps are able to generate a profile of the apps users.

Add in geographic information such as Uber, Google maps, and services which track the weather and it becomes easy to see where one lives, where they work, what places they visit, and the frequency in which they do so. These services establish your social status by connecting the dots. It's not illogical to be able to also get a sense of someone's socioeconomic level and political leanings from these data as they convey zip codes and physical places that are visited as well. Apps such as Google and Amazon, et al., collect what consumers buy and use it as key data to improve the robustness of their profit margin and establish socioeconomic status as good indicators of education, age, and household size. Ingeniously, these services enable price discrimination on an unprecedented scale.

Apps and the internet essentially create the ultimate marketplace where companies can sell the same item to different people at different prices based on the profile of each individual consumer.[39] Commercial entities and the industry argue that collecting this information allows them to deliver better, more tailored services for the user. Although that is a reasonable argument

https://www.today.com/news/appitypes-you-are-what-you-app-study-finds-wbna41625761.

[39] Charles J. Wheelan, *Naked Economics: Undressing the Dismal Science*, 1st ed. (New York: Norton, 2002), 18.

for this type of data collection, this approach does not reveal everything that they do with the data. Much less evident is the fact that the data collected from each user and their household and/or social network allows them to build a virtual and detailed personal profile of everyone who uses them and who might use their products in the future.

Implications for the Military Consumer

Every time a phone number is used in conjunction with store purchases a record is generated. Using a military ID at the Commissary also informs the commissary what products are purchased and by whom. These data are collected all for the improved experience of the buyer or user, but who else benefits from such data? "There's an old truism that's popular among privacy advocates: "If you're not paying, you're the product." Your age, interests, purchasing habits, frequented locations, health, and social map are all valuable pieces of information that comprise a digital shadow, which can be packaged, bundled, and sold to the highest bidder."[40]

Impact on the Military and National Security

Operational security (OPSEC) is a constant concern of military operations. All military personnel receives numerous inoculations, annual training, refreshers, and reminders in briefings throughout their tenure. Their medical record is particularly sensitive because of the unique set of inoculations given strictly to the military vs civilian populations. These inoculations (e.g. anthrax, Congo fever, malaria, etc.) leave a genetic marker that makes them identifiable as military personnel regardless of location and uniform. This genetic marker also makes them an easy target for the bioterrorist adversary. The military is engrained largely not to communicate

[40]Lisa Gutermuth, "How to Understand What Info Mobile Apps Are Collecting About You," *SLATE, NEW AMERICA, AND ASU*, February 24, 2017, http://www.slate.com/articles/technology/future_tense/2017/02/how_to_understand_what_info_mobile_apps_collect_about_you.html.

timing or the physical locations of troop movements related to military operations. However, the fact remains, mobile devices are as ubiquitous as a wallet, and there are likely protocols that can be developed to watch when normally active users become silent which can also be an indicator of activities of interest to adversaries. The Enigma code breakers of WWII learned the signal patterns of German enigma operations just by the pattern of their keystrokes. They could tell whose shift it was and deduced where they were located just by the pattern of typing. Similarly, the pattern of accessing apps or not accessing apps might similarly be revealed to adversaries.

But what of everyday life when military personnel and their families are not deployed? These same apps are busy building profiles of personnel and their entire families which can be targeted for all sorts of activities regardless of deployment status. Identity theft may be the least of concerns, as it's likely more advantageous to create surrogate profiles to interact with users' contacts and be those users rather than merely steal from one.

What if Stalin or Hitler would have had access to such data? The sheer volume of information allows sinister actors to hide in plain sight posing as a friend or casual associate. The same data that create convenience and serve user preferences could easily be misused by the state and their agents to target, control and even eliminate a particular profile of users. Vitals, intelligence quotients, emotional states, professional and private networks became extremely accurate indicators of people and continue to be refined over time. Location data capture networks of interactions with other contacts even children, places of home and business all which can be tracked and monitored.

Another possibility is for this shadow profile to mimic the user's presence even if that were not the case. People just don't get together in person often enough or when they do make plans, they often change or cancel them because of the ease with which it can be done. A particular

nefarious actor could target profiles with specific IQs, special needs, those on government assistance, or those with activist tendencies. Adversaries could use these profiles to target families and their children or blackmail individuals with any number of demands. They could also use these data to help shape a society that will be easily controlled, constantly surveilled and monitored, and shaped according to the leader's political and financial advantage.

This technology is already being used in China to monitor and control Uighurs (the predominately Muslim, Turkic speaking ethnic group) in Northwestern China. Scores of video surveillance cameras track individual movements and police checkpoints scan IDs and phones and even scan pupils. "This personal information, along with biometric data, resides in a database tied to a unique ID number. The system crunches all of this into a composite score that ranks you as "safe," "normal" or "unsafe." Based on those categories, you may or may not be allowed to visit a museum, pass through certain neighborhoods, go to the mall, check into a hotel, rent an apartment, apply for a job or buy a train ticket. Or you may be detained to undergo re-education, like many thousands of other people."[41]

China also intends to use the aforementioned surveillance machinery to rank its citizenry according to social credit much like a credit report does for credit worthiness. "The exact methodology is a secret — but examples of the behaviors that will be monitored are driving and purchasing habits, and the ability to follow the rules."[42] The implications will dictate what services will be available to an individual and will even restrict them from some services all together.

---

[41] James Millward, "What It's Like to Live in a Surveillance State*," The New York Times*, February 3, 2018, https://www.nytimes.com/2018/02/03/opinion/sunday/china-surveillance-state-uighurs.html.

[42] Alexandra Ma, "China Has Started Ranking Citizens with a Creepy 'Social Credit' System — Here's What You Can Do Wrong, and the Embarrassing, Demeaning Ways They Can Punish You," *Business Insider*, April, 8, 2018, http://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4.

If Hitler or Stalin had these capabilities history might have turned out differently but as we see in China, "Tibetans know well this hard face of China. Hong Kongers must wonder: If Uighur culture is criminalized and Xinjiang's supposed autonomy is a sham, what will happen to their own vibrant Cantonese culture and their city's shaky "one country, two systems" arrangement with Beijing? What might Taiwan's reunification with a securitized mainland look like? Will the big-data police state engulf the rest of China? The rest of the world?"[43] This dystopian future is arriving if it has not arrived already.

Discussion

Just as Monu Bedi argues, to understand the historical context and unique contours of each [disclosure and privacy] doctrine[s] so that, "For prudential reasons, we must strive for a logical and cautious application of these principles that is firmly grounded in prior precedent. Otherwise, courts as well as scholars risk muddying the waters and, in turn, making unnecessarily overly broad or erroneous conclusions on important privacy matters." [44] The same topology can be argued as a need to understand the contours around privacy to include privacy norms and terms of use agreements as well as societal ethics and collecting personal data. This project perhaps can contribute to that end but focuses more on a few near-term solutions aimed at the definition and social norms around privacy.

Discussing ethical issues is difficult because the context for the argument is often assumed to be clear, that those engaging in the discussion are relatively on the same "page" with respect to the interpretation of the facts of the argument, and there is some assumed sense of a common understanding of the consequence of the dilemma in question. This is hardly, if ever, the actual

[43] Millward, *The New York Times*, February 3, 2018.
[41] Bedi, *The William and Mary Bill of Rights Journal*, 494.

case because people are varied in all aspects of experience and interpretation of life. Changing the social norms around terms of use agreements is a daunting task and would take a significant amount of time. Any viable solution in terms of social norms or legislation needs to define the boundary between ownership, use, and control and balance individual privacy between an individual and the security of society, so establishing definitions for key terms such as privacy is a useful first step.[45]

It is difficult to imagine how something so trivial as terms of use or privacy agreements could be so dangerous or enable paranoid outcomes such as threatening the U.S. military or abducting people without really knowing they're gone. But, "[T]he significance of privacy policies greatly exceeds the attention paid to them: these documents are binding legal agreements between website operators and their users, and their opaqueness is a challenge not only to Internet users but also to policymakers and regulators."[46] Policymakers that are influenced by the significant money discussed in the opening of this essay no less. These agreements are ignored by users because, like mortgage documents, they tend to be long and difficult to understand.[47] It also does not help that the average citizen takes for granted they live in a society with governance backed by the rule of law. How then can users be expected to agree and thus consent to accept technologies where the full understanding and outcomes of their use are unknown? More importantly, when individuals surrender their privacy, they also unwittingly surrender their individual freedom as they have allowed others to dictate their choices.

---

[45] Rincon, *Revista Signoy Pensamiento*, 288.

[46] Shomir Wilson, et. al.,"The Creation and Analysis of a Website Privacy Policy Corpus, the Usable Privacy Project." In *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics*, edited by Katrin Erk and Noah A. Smith, 1338. Berlin: Association for Computational Linguistics, August 2016. https://www.usableprivacy.org/data accessed 4/18/2018.

[47] Wilson, et. al., In *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics*, 1330.

These questions are not purely legal, either. They present confluent ethical and policy issues. The interests of the public in advancing and sustaining national security must be weighed in comparison with the private interest in protecting individual rights."[48] Privacy and Terms of Use Agreements should follow the Aristotelian considerations: Is the story coherent? Is it simple enough to be processed? Can it be remembered? Is it easy to transmit? If believed, will it motivate appropriate action?[49] "The ethical-legal issues, questions, and problems demand attention before these technologies become operational. That will enable a determination as to what legal standards may be viable—or should be developed—to govern (1) the informal or formal pressures placed on individuals to participate in using such technology, (2) the disclosures required for informed consent, (3) the level of care taken to protect individuals from harm, and (4) the liability that parties bear when individuals using such cutting-edge neurotechnologies are harmed."[50]

There are several options that could be pursued which would have a significant impact in taking charge of our own data. Recall the findings from the grand traditions: virtue theorists would likely recommend treating terms of service and privacy agreements as contracts of trust; deontologists might recommend changing the current default option of most app accounts from opting out to choosing to *opt in*; and utilitarianists would accept the current paradigm as long as the punishment for violations were severe enough to maintain the happiness of society once an offender was caught. More importantly, these inconsistencies again highlight the need to

[48] Giordano, *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns*, 134.

[49] Giordano, *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns*, 283.

[50] Jonathan D. Moreno, *Undue Risk: Secret State Experiments on Humans,* New York: W.H. Freeman, 2001, Quoted in James J. Giordano, *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns,* Boca Raton, Florida: CRC Press, 2015, 137.

.

understand the boundaries between privacy as examined through the individual, society, and the existing consequences so that future threats can be addressed with ethical solutions. *Individuals should be provided with a clear and concise explanation of their privacy rights, as well as the potential risks associated with the use of systems and apps. Like a mortgage loan, this information must be fully disclosed before consent is given. Identification of the risks must be clearly presented to the user.*

A Definition of Privacy

Kristen Martin discusses privacy as a social contract and provides a useful definition for the argument here:

> "[T]he most thoroughly context-dependent approach to privacy is perhaps Nissenbaum's privacy as contextual integrity (2004, 2009). Nissenbaum views privacy as the negotiated agreements about how information is accessed and distributed. Maintaining privacy norms entails the "information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it" (Nissenbaum 2004, p. 101). In doing so, Nissenbaum ties privacy expectations to norms within specific contexts and incorporates both the relationship and the situation in defining privacy."[51]

This definition seems to cover the waterfront in a way that establishes norms for societal considerations while giving flexibility for the user to consider how the information is used and therefore how they agree for these data to be accessed. It is this exact agreement that embodies informed consent so is used to support that exact framework in the context of Internet research ethics.

[51] Helen Nissenbaum, Privacy as Contextual Integrity, *Washington Law Review* 79(1), 2004: 119-158, Quoted by Kirsten E Martin, "Diminished Or just Different? A Factorial Vignette Study of Privacy as a Social Contract, "*Journal of Business Ethics* 111, no. 4 (2012): 519-539, http://www.jstor.org/stable/23324816.

Consent—a Waiver of Normative Expectations

A strong foundation for consent was established with the Nuremberg Code. The Ten points ("The Nuremberg Code"; Germany 1949) hold that the voluntary consent of the human subject is absolutely essential. This means that the person involved should have the capacity to give legal consent; should be so situated as to be able to exercise free power of choice, without the invention of any element of force, fraud, deceit, duress, over-reaching, or other ulterior form of constraint or coercion; and should have sufficient knowledge and comprehension of the elements of the subject matter involved, so as to enable him/her to make an understanding and enlightened decision.[52]

The concept of informed consent as applied from the medical field requires an opportunity for one to learn and think about the pros and cons of a treatment before agreeing to it. In medicine, a signed informed consent form unlike an agreement to use an app is not necessarily valid until the process to learn and think about the treatment is exercised.[53] How can an informed decision be made if all aspects of the benefits, risks, and consequences are not adequately understood? This process is compromised with respect to the concept of privacy and data collection since "…market interactions involving personal data often take place in the absence of individuals' fully informed consent. Furthermore, specific heuristics may profoundly influence consumers' privacy decision making and ethics and social norms change with technology."[54] The

[52] Giordano, *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns*, 140.

[53] *The American Cancer Society*, "What Is Informed Consent and What Does it Mean?" Canver.org. Accessed on March 31, 2018, https://www.cancer.org/treatment/finding-and-paying-for-treatment/understanding-financial-and-legal-matters/informed-consent/what-is-informed-consent.html.

[54] Acquisti, *Journal of Economic Literature*, 444.

only way the norms of acceptance have a chance of being changed is to better ensure people become informed and have the opportunity to interactively learn.

The medical field has well-developed case law in dealing with ethical issues related to patient care. It is also a field that most people have some working knowledge of the difficulties in navigating a highly specialized field where the consequences of choosing incorrectly can be quite high. There are strong parallels with the topic of privacy and data collection and the medical field where informed consent is the foundation of agreements between patients and doctors. Like the medical field, a high degree of asymmetry in knowledge exists between users and developers in much the same way as between patients and doctors. But there are major differences between medical ethics and data collection such as the level of perceived risk and the Hippocratic oath that warrants a willingness of the individual to become informed and the doctor to protect the patient that are largely absent in this type of interaction. These differences are behind Dr. Flick's "waiver of normative expectations."[55]

Facebook and its emotional manipulation study with Cornell University already set precedent for applying informed consent to data analytic research. "[R]esearchers at Facebook tweaked what hundreds of thousands of users saw in their news feeds, skewing content to be more positive or negative than normal in an attempt to manipulate their mood."[56] Neither the terms of service agreements nor Cornell University had what Catherine Flick describes as, "[S]ufficient ethical oversight and neglected in particular to obtain necessary informed consent from the participants in the study." She goes on to argue that, "[A] reasonable shift could be made from

[55] Catherine Flick, "Informed Consent and the Facebook Emotional Manipulation Study," *Research Ethics* Vol. 12(1), (2016): 19, http://journals.sagepub.com/doi/pdf/10.1177/1747016115599568.

[56] Gail Sullivan, "Cornell Ethics Board Did Not Pre-Approve Facebook Mood Manipulation Study," *The Washington Post,* July 1, 2017, https://www.washingtonpost.com/news/morning-mix/wp/2014/07/01/facebooks-emotional-manipulation-study-was-even-worse-than-you-thought/?noredirect=on&utm_term=.9dbc99d9c641.

traditional medical ethics 'effective consent' to a 'waiver of normative expectations', although requires much-needed changes to the company's standard practice."[57]

The change to company standard practice would have to address disclosure and require being upfront with the user about the intent of the research. Moreover, the terms of service agreement would need to be more easily understood, i.e., "Facebook can, in fact, improve their terms of service in such a way that the expected norms are included as part of the base standard, but that expectations that need to be waived are communicated effectively and consented to (either negatively or positively) by the user."[58]

International Law

Informed analysis of the ethical and legal issues requires an integrated approach that looks to include norms embraced in international law.[59] Ralph Schroeder and Jamie Halsall in a summary article interviewed several business leaders and found,

> "[T]here is a shared sense that the existing regulatory environment [i.e., big data policies] fail to be transparent, clear, fair and consistent. […] One area of particular friction surrounds the issue of privacy and personal data. The law has lagged behind both the growth in personal data use and developments in technical and statistical anonymization techniques. There is also a lack of standardization of privacy practices across jurisdictional boundaries. These failings are reflected in a somewhat piecemeal response to the personal data issues in industry, and there is still no accepted standard for how such issues should be treated—or even what the appropriate definition of personal data should be. Voluntary standards or codes of conduct, according to interviewees, would be a good first step given the likely intractability of a truly global privacy regulation."[60]

[57] Flick, *Research Ethics*, 14.
[58] Flick, *Research Ethics*, 19.
[59] Giordano, *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns*, 138.
[60] Ralph Schroeder and Jamie Halsall, "Big Data Business Models: Challenges and Opportunities," *Cogent Social Sciences* 2, no. 1 (2016): 11, DOI: 10.1080/23311886.2016.11669242016.
.

Mobile applications and the internet are individual resources that are used globally. Thus, data collected as a byproduct of these activities are also regulated according to the laws in each country. Lasting protections would need to consider and address these realities.

In the U.S. it is largely up to the consumer to understand the consent that is given through privacy policies and terms of agreements since there exists a patchwork of regulation and entities responsible for regulating this space. However, there are other countries around the world that recognize the right to privacy and are leading the way in protecting the consumer that may ultimately change practices in the U.S. The EU recently passed General Data Protection Regulation (GDPR) which goes into effect May 2018 and is, "[I]ntended to harmonize privacy laws for all of the members of the EU. The law emphasizes consent, control, and demands clear explanations to users so they know how data is collected on them."[61]

The Privacy Corpus

Another option is to fight fire with fire or in this case, fight algorithms with algorithms. The very same machine learning algorithms are being looked to automatically make privacy easier to understand and automatically update as fast as the technology is developed. "One proposed alternative to the status quo is to automate or semi-automate the extraction of salient details from privacy policy text, using a combination of crowdsourcing, natural language processing, and machine learning."[62] A team from Carnegie Mellon is currently building and scaling up a privacy corpus to help Internet users understand online privacy practices. By using law students, the team analyzed 115 privacy policies and were able to demonstrate the feasibility of partly automating

[61] Nitasha Tiku, "Europe's New Privacy Law Will Change the Web, and More," *WIRED*, March 19, 2018, https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more/.

[62] Wilson, et. al., In *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics*, 1330.

the annotation process with several machine learning toolkits. While it was only a demonstration, the results reveal the complexity of these documents. [63] A tool like this may one day allow the user to answer a few questions designed to understand how they value privacy and then automatically identify apps that are inconsistent with these preferences. At a minimum, these efforts would provide near-term solutions until the more conservative privacy paradigm of the EU is adopted elsewhere.

Conclusion and Future Work

The ubiquitous nature of the digital world and the voluminous records of user behaviors within that world gives birth to a digital model of you with your unique characteristics, interests, values, and beliefs. This model becomes more robust over time as more and more inputs are generated by the user. This presents numerous threats to the individual, to society and to the organizations such as the U.S. military as described here. Privacy is central to the issue at hand—terms of use agreements are legally binding agreements that give permission to access these data, thus an argument is made for treating these agreements with the same gravity as informed consent receives in the field of medicine.

The degradation of trust in a society as one can imagine has ill effects too many to number since trust underscores the goodwill between the individual and the collective society. The concept of privacy and its erosion are a mere subset of this goodwill; however, I argue an erosion of privacy is just as, if not more threatening since society chooses to define privacy, rather than trust, under the law so should go to great lengths to ensure its protection. There is a fundamental discrepancy manifested in the consequences of informed consent of the medical field and the

[63] Wilson, et. al., In *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics*, 1338.

case here with data collection and privacy. Namely, damage to an individual's health is much easier to measure, "see," and empathize with than damages associated with a violation of the latter which is felt more by the society. This paper supports the waiver of normative expectations model argued by Dr. Flick to protect users, but it begs the question, is informed consent, or even a waiver of normative expectations, really correct constructs for managing these relationships either?

Throughout the discussion, particularly when discussing the three grand ethical traditions, this work illustrates the need for setting and keeping a common frame of reference on privacy since there are clear dangers to the individual, to society, and to the state. This paper introduces ethics into a discussion that is evidently nebulous in terms of individual rights, commercial interests, and judicial precedent as a way to further convey these dangers to the individual in a relatable manner. Thus, a topology that establishes the contours between privacy and the ethics of collecting personal data, much in the same way that Monu Bedi does for disclosure and privacy doctrine, is a logical next step to the discussion started here.

Bibliography

Acquisti Alessandro, Curtis Taylor, and Liad Wagman. "The Economics of Privacy." *Journal of Economic Literature.* 54(2). 2016. 442-492.

Al Jazeera News. "Cambridge Analytica and Facebook: The Scandal So Far." News Privacy & Surveillance. March 28, 2018. https://www.aljazeera.com/news/2018/03/cambridge-analytica-facebook-scandal-180327172353667.html.

Anderson-Gold, Sharon. "Privacy, Respect and the Virtues of Reticence in Kant." *Kantian Review*. 15(2). 2012. 28-42.

Arango, Tim. "The Cold Case That Inspired the 'Golden State Killer' Detective to Try Genealogy." *The New York Times.* May 3, 2018. https://www.nytimes.com/2018/05/03/us/golden-state-killer-genealogy.html.

Bedi Monu. "The Fourth Amendment Disclosure Doctrines." *The William and Mary Bill of Rights Journal.* 26(2). 2017. 461-494. Retrieved from https://search-proquest-com.usnwc.idm.oclc.org/docview/2023675687?accountid=322.

Downing, Douglas. *Dictionary of Mathematical Terms*. 2nd ed. New York: Baron's Educational Series. 1995.

Doyle, Tony. "Privacy and Perfect Voyeurism." *Ethics and Information Technology 11*(3). 2009. 181-189. http://dx.doi.org.usnwc.idm.oclc.org/10.1007/s10676-009-9195-9 Retrieved from https://search-proquest-com.usnwc.idm.oclc.org/docview/222251629?accountid=322.

Flick, Catherine. "Informed Consent and the Facebook Emotional Manipulation Study." *Research Ethics.* Vol. 12(1), (2016): 14–28. http://journals.sagepub.com/doi/pdf/10.1177/1747016115599568.

Fox, Maggie. "What You're Giving Away with those Home DNA Tests." *NBC Health News*, updated Nov 30, 2017. https://www.nbcnews.com/health/health-news/what-you-re-giving-away-those-home-dna-tests-n824776.

Giordano, James J. *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns*. Boca Raton, Florida: CRC Press, 2015.

Gutermuth, Lisa. "How to Understand What Info Mobile Apps Are Collecting About You." *SLATE, NEW AMERICA, AND ASU*, February 24, 2017. http://www.slate.com/articles/technology/future_tense/2017/02/how_to_understand_what_info_mobile_apps_collect_about_you.html.

Hempel, Jessi. "Social Media Made the Arab Spring but Couldn't Save It." *WIRED*, January 26, 2016. https://www.wired.com/2016/01/social-media-made-the-arab-spring-but-couldnt-save-it/.

Henke, Nicolaus, Bughin Jacques, Michael Chui, James Manyika, Tamim Saleh, Bill Wiseman, and Guru Sethupathy. *The Age of Analytics: Competing in a Data-Driven World*. McKinsey Global Institute Report, 2016. https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/the-age-of-analytics-competing-in-a-data-driven-world.

Hoback, Cullen. *Terms and Conditions May Apply*, Documentary Film, 2013. Slamdance Film Festival, Park City, Utah, USA. 2013.

James, Josh. "Data Never Sleeps 5.0." *Domo Blog*. Last modified July 25, 2017. http://bit.ly/2uvd4nH.

Ma, Alexandra. "China Has Started Ranking Citizens with a Creepy 'Social Credit' System — Here's What You Can Do Wrong, and the Embarrassing, Demeaning Ways They Can Punish You." *Business Insider*, April, 8, 2018. http://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4.

Martin, Kirsten. "Understanding Privacy Online: Development of a Social Contract Approach to Privacy." *Journal of Business Ethics.* 137(3). Sep 2016, 2016. 551-569. https://search.proquest.com/docview/1811874287?accountid=322.

Millward, James. "What It's Like to Live in a Surveillance State*." The New York Times*, February 3, 2018. https://www.nytimes.com/2018/02/03/opinion/sunday/china-surveillance-state-uighurs.html.

Moreno, Jonathan D. *Undue Risk: Secret State Experiments on Humans.* New York: W.H. Freeman, 2001. Quoted in James J. Giordano, *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns*. Boca Raton, Florida: CRC Press, 2015, 267-71.

Mulvey, Jeanette. "'Appitypes': You Are What You App, Study Finds." *TechNewsDaily,* February 16, 2011. https://www.today.com/news/appitypes-you-are-what-you-app-study-finds-wbna41625761.

Nevala, Kimberly. *The Machine Learning Primer*. Cary, NC: SAS Institute, 2017. https://s3.amazonaws.com/baypath/files/resources/machine-learning-primer-108796.pdf.

Nissenbaum, Helen. Privacy as Contextual Integrity. *Washington Law Review* 79(1), 2004. Quoted by Kirsten E Martin, "Diminished Or just Different? A Factorial Vignette Study of Privacy as a Social Contract, "*Journal of Business Ethics* 111, no. 4 (2012): 519-539. http://www.jstor.org/stable/23324816.

Peltz, James Joseph. "Demonstrating Predictive Confidence for a Paradigm Dissolver Model using Methods for Evaluating Higher Order Moments: A "Case Study" for Nuclear Nonproliferation." (PhD diss., Karlsruhe Institute of Technology, 2016. http://primo.bibliothek.kit.edu/primo_library/libweb/action/search.do.

Plato, *The Last Days of Socrates*. London Penguin Group, 2003.

Recorded Future. “Threat Intelligence Machine.” http://www.recordedfuture.com/technology/. Accessed on March 31, 2018.

Rincon, Valencia and Juan Carlos. "Internet and Surveillance. The Challenges of Web 2.0 and Social Media." *Revista Signoy Pensamiento*, Vol. 31, Núm. 61 (2012): 191-193.

Schroeder, Ralph and Jamie Halsall. “Big Data Business Models: Challenges and Opportunities.” *Cogent Social Sciences*, 2(1). 2016. 1-15. DOI: 10.1080/23311886.2016.11669242016.

Strauss, Valerie. “Personal Data Is Collected on Kids at School All the Time. Here’s Help for Parents to Protect Children’s Privacy.” *The Washington Post*, May 16, 2017. https://www.washingtonpost.com/news/answer-sheet/wp/2017/05/16/personal-data-is-collected-on-kids-at-school-all-the-time-heres-help-for-parents-to-protect-childrens-privacy.

Sullivan, Gail. “Cornell Ethics Board Did Not Pre-Approve Facebook Mood Manipulation Study.” *The Washington Post*, July 1, 2017. https://www.washingtonpost.com/news/morning-mix/wp/2014/07/01/facebooks-emotional-manipulation-study-was-even-worse-than-you-thought/?noredirect=on&utm_term=.9dbc99d9c641.

The American Cancer Society. “What Is Informed Consent and What Does it Mean?” Canver.org. Accessed on March 31, 2018. https://www.cancer.org/treatment/finding-and-paying-for-treatment/understanding-financial-and-legal-matters/informed-consent/what-is-informed-consent.html.

The New York Times. “Mark Zuckerberg Testimony: Senators Question Facebook’s Commitment to Privacy.” Politics, April 10, 2018. https://www.nytimes.com/2018/04/10/us/politics/mark-zuckerberg-testimony.html.

Tiku, Nitasha. “Europe’s New Privacy Law Will Change the Web, and More.” *WIRED*, March 19, 2018. https://www.wired.com/story/europes-new-privacy-law-will-change-the-web-and-more/.

U.S. Const. Amend. IV.

Wheelan, Charles J. *Naked Economics: Undressing the Dismal Science*. 1st ed. New York: Norton, 2002.

Wilson, Shomir, Florian Schaub, Aswarth Abhilash Dara, Frederick Liu, Sushain Cherivirala, Pedro Giovanni Leon, Mads Schaarup Andersen, Sebastian Zimmeck, Kanthashree Mysore Sathyendra, N. Cameron Russell, Thomas B. Norton, Eduard Hovy, Joel Reidenberg, and Norman Sadeh. “The Creation and Analysis of a Website Privacy Policy Corpus, the Usable Privacy Project.” In *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics*, edited by Katrin Erk and Noah A. Smith, 1330-1340. Berlin:

Association for Computational Linguistics, August 2016. https://www.usableprivacy.org/data accessed 4/18/2018.