Washington Journal of Law, Technology & Arts

Volume 15 | Issue 1 Article 2

12-13-2019

Featurization and the Myth of Data Empowerment

Nur Lalji

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 15, ISSUE 1 FALL 2019

FEATURIZATION AND THE MYTH OF DATA EMPOWERMENT

Nur Lalji[*]

CITE AS: N. LALJI, 15 WASH. J.L. TECH. & ARTS 1 (2019)

https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1299&context=wjlta

ABSTRACT

Every day, we make a series of tradeoffs between privacy and convenience. We may check our email, post on social media, use the free Wi-Fi in public spaces, or take our cellphones with us wherever we go without a clear understanding of what information we are giving away when we do so. Increasingly, we are seeing products that claim to defy this opaqueness associated with big data and put users at the helm of their information. These "featurized" products wrap themselves in a data empowerment narrative, but ultimately erode individual privacy in new ways, sometimes even capitalizing on it. This article seeks to explore the concept of featurization further—where it came from, what it is, and how featurized products are currently being regulated. The article will end by proposing some recommendations for balancing the innovation that featurization can bring while ensuring individuals' privacy rights are adequately protected.

[*]A huge thank you to Professor Anupam Chander for all of his help and guidance in writing this article, and to all of the *Washington Journal of Law, Technology & Arts* editors for their instrumental help in getting this work published. This Article does not represent the views of the organization with which the author is affiliated.

TABLE OF CONTENTS

INTRODUCTION

"It's not a bug, it's a feature." The pithy catchphrase coined by programmers to reframe mechanical defects as intentional and desirable[1] also deftly defines the transition from big data's scary opacity to a new era of transparency and access. What was once a bug—the unknowable and seemingly unending troves of data that

[1] Nicholas Carr, *'It's Not a Bug, It's a Feature.' Trite—or Just Right?*, WIRED (Aug. 19, 2018), https://www.wired.com/story/its-not-a-bug-its-a-feature/.

companies have collected about us—is now its feature, by making users' data trails visible, accessible, and interactive. This "featurization" of data has been characterized as the antidote to big data's shadowy tendencies—a way to bring companies' data collection and use practices into the sunlight, and provide individuals with tangible value.[2] It refers both to the new products that allow individuals to track and analyze their own data, and the secondary features provided as a quid pro quo for data collection.

Several companies across many different sectors offer featurized products. Genetic companies like 23andMe offer individual reports on ancestry and genetic health risks.[3] Financial planning apps like Mint help users create budgets and remind them to pay their bills on time.[4] Smart thermometers like Nest provide users with information about their daily movements and routines in addition to helping them save money on their utility bills.[5] Period tracking apps like Flo and Ovia provide women with insight into their menstrual health and help them plan and track their pregnancies.[6] All of these applications purport to empower individuals by enabling them to gain personal knowledge through data collection and achieve individual goals.

However, while the marketing of these products provides a small window into companies' data use practices, they also obscure how individuals' data can be used in ways that are adverse to their interests. Moreover, these behind-the-scenes practices are often enhanced by the interactive and accessible features these companies offer. 23andMe, for example, recently sold the exclusive rights to search through their customer data for drug targets to

---

[2] *See* Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 242-43 (2013).

[3] *Compare Our DNA Tests*, 23ANDME, https://www.23andme.com/compare-dna-tests/ (last visited Apr. 26, 2019).

[4] *Bill Tracking: Online Monthly Bill Tracking & Reminders*, MINT, https://www.mint.com/how-mint-works/bills#toc (last visited Apr. 26, 2019).

[5] *Overview*, NEST, https://nest.com/thermostats/nest-learning-thermostat/overview/ (last visited Apr. 24, 2019).

[6] *See, e.g.*, Tehrene Firman & Samantha Lefave, *The Best Period Tracker Apps that Belong on Your Phone*, REDBOOK (July 31, 2018), https://www.redbookmag.com/body/g19091742/best-period-tracker-apps/.

pharmaceutical company GlaxoSmithKline.[7] Likewise, period-tracker apps have come under fire for sharing users' personal information with advertisers and other third parties.[8]

The data collected by these products, particularly in sensitive industries such as finance and health, may harm individuals in several key respects, including discrimination, economic loss, and increased vulnerability to data breaches. These practices also create large databases of extremely personal information that law enforcement may be able to access without ever having to notify affected individuals.[9] Additionally, by providing direct-to-consumer services, companies may be able to skirt the more stringent sectoral privacy laws because they do not fall under the traditional conception of a covered entity.[10]

This paper will explore the current era of big data: the countless products that encourage individuals to engage with data about themselves and how that interaction leads to harms that manifest themselves over the long term. Although much has been written about the privacy and security concerns related to the Internet of Things, as well as data tracking products in particular industries, there is currently limited literature on the harms both unique to and exacerbated by featurization. Part I of this article will provide the reader with a framework for thinking about featurization and its benefits. Part II will summarize the state of consumer privacy laws

---

[7] *See* Megan Molteni, *23andMe's Pharma Deals Have Been the Plan All Along*, WIRED (Aug. 3, 2018), https://www.wired.com/story/23andme-glaxosmithkline- pharma-deal//.

[8] *See* Sarah Burke, *Your Menstrual App Is Probably Selling Data About Your Body,* VICE (May 11, 2018), https://broadly.vice.com/en_us/article/8xe4yz/menstrual-app-period-tracker-data-cyber-security.

[9] *See, e.g.*, Salvador Hernandez, *One of the Biggest At-Home DNA Testing Companies Is Working with the FBI*, BUZZFEED NEWS (Jan. 31, 2019), https://www.buzzfeednews.com/article/salvadorhernandez/family-tree-dna-fbi-investigative-genealogy-privacy; Russell Brandom, *Why Facebook is Beating the FBI at Facial Recognition*, THE VERGE (July 7, 2014), https://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition.

[10] *See, e.g.*, Katherine Drabiak, *Caveat Emptor: How the Intersection of Big Data and Consumer Genomics Exponentially Increases Informational Privacy Risks*, 27 HEALTH MATRIX 143, 160 (2017).

in the United States. Part III will assess the harms that featurization poses and analyze whether existing privacy laws at the federal or state level offer any meaningful protections. Finally, Part IV of this article will offer suggestions on how to maintain value and utility while providing baseline privacy and security protections.

I. FEATURIZATION IN CONTEXT

In 2012, a man stormed into a Minneapolis Target to complain that the store was mailing coupons for baby and maternity items to his daughter.[11] He found it inappropriate that the store was mailing her these advertisements while she was still in high school. Target, however, had just predicted the pregnancy before his daughter had let the family know. This story became infamous for representing how companies' use of big data can quickly cross privacy boundaries[12]—and Target is not the only company to have committed a big data faux pas.[13]

As more stories emerged highlighting the negative consequences of big data, public perception of private data collection shifted.[14] By 2014, 91% of adults agreed or strongly agreed that consumers no longer had control over how companies used or collected their personal information, while 64% believed the

---

[11] Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#12cc321c6668.

[12] *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp.

[13] *See, e.g.*, Ben Goldacre, *When Data Gets Creepy: the Secrets We Don't Realise We're Giving Away*, THE GUARDIAN (Dec. 5, 2014), https://www.theguardian.com/technology/2014/dec/05/when-data-gets-creepy-secrets-were-giving-away.

[14] *See, e.g.*, MARY MADDEN, PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA 1-2 (2014), https://www.pewinternet.org/2014/11/12/public-privacy-perceptions/; Maggie McGrath, *Target Data Breach Spilled Info on As Many As 70 Million Customers*, FORBES (Jan. 10, 2014), https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#104d23c8e795.

government should do more to regulate advertisers.[15] Moreover, the survey indicated that people wanted more of a say as to how their data was being used; 93% said that being in control of who may access information about them was "very important."[16]

The concept of featurization was born out of the growing disenchantment with big data. It was first proposed as a way to subvert the opacity of companies' data collection practices, by making data a "consumer-side feature of products and services."[17] Simply put, featurization creates an intentional link between consumers' data and companies' data collection and processing practices by returning some of that value to the consumer. Think of an ancestry composition report by 23andMe, which distills an individual's heritage into neat and distinct categories, or, the Nest Learning Thermostat, which provides a breakdown of users' household activity habits; both of these products prominently display the data they are collecting from users and offer them insight they may have otherwise been unable to identify. These types of products and services are now widely available across various sectors—from medicine to social media.

The problem with featurization, however, is that it merely provides a window into the data a product collects rather than the full picture. Under the typical featurization paradigm, users are only privy to some of the data collected and only some of the ways the data may actually be used. In this way, access has been falsely equated with full transparency. For example, although Nest allows users to see the data collected about them through user activity reports, Nest had not initially been so forthright about whether its user data would be combined with Google's, once it had been

---

[15] Madden, *supra* note 14, at 30.

[16] Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RES. CTR. (May 20, 2015), https://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

[17] The term "featurization" was first coined by Omer Tene and Jules Polonetsky in their seminal piece, *Big Data for All.* This process, Tene and Polonetsky suggest, should be offered up as a "quid pro quo for looser data collection and minimization restrictions." *See* Tene & Polonetsky, *supra* note 2, at 263-64.

acquired.[18] Similarly, while 23andMe extols the types of information it can make available to users about their DNA, it may bury how long it will keep users' data, or what it might do with the data afterwards, even after a user requests its deletion, in the middle of the privacy policy.[19] Featurization thus exacerbates some of the harms already posed by big data, and, in certain cases, creates new ones.

This section will break up products that "featurize" data into two types: those that function through self-surveillance, and those that provide users access to their data as a secondary benefit, and offer some examples in each category. Then, it will assess how the differences might play out under existing laws and regulations.

A. Primary Featurization

Primary featurization is quintessentially about self-surveillance. The express purpose of primary featurization products is to process and featurize users' data; thus, the trade-off between privacy and insight is made apparent from the beginning of the user's relationship with the product.[20] More strongly put, these products are *predicated* on lessened privacy interests in return for the value these products purport to offer. Users are subsequently comfortable allowing themselves to be surveilled to a certain degree in order to obtain the benefits that the product offers.

The healthcare industry is saturated with primary featurization products. The abundance of these products can be traced, in part, to the popularity of the "quantified self" movement, which promotes tracking health-related data about oneself as a means to further one's mental, physical, and emotional health.[21] Consequently, the

---

[18] Casey Johnston, *What Google Can Really Do with Nest, or Really, Nest's Data*, ARS TECHNICA (Jan. 15, 2014), https://arstechnica.com/information-technology/2014/01/what-google-can-really-do-with-nest-or-really-nests-data/.

[19] *See, e.g.*, Peter Pitts, *The Privacy Delusions of Genetic Testing*, FORBES (Feb. 15, 2017), https://www.forbes.com/sites/realspin/2017/02/15/the-privacy-delusions-of-genetic-testing/#898eb721bba5.

[20] *See* Kang et al., *Self-Surveillance Privacy*, 97 IOWA L. REV. 809, 813-15 (2012).

[21] Although the movement began in the 1970s, the term was coined by two Wired Magazine editors, Gary Wolf and Kevin Kelly, in 2007. The movement

innumerable products that featurize health-related data include personal genomics testing; diagnostic apps; and fitness, diet, and menstrual trackers, that monitor everything from heart rate, calories burned, number of steps, body temperature, quality and length of sleep, menstrual cycles, and emotional patterns. To highlight the types of sensitive personal information these types of products collect, some examples are described in more detail below.[22]

1. Ovulation and Menstrual Trackers

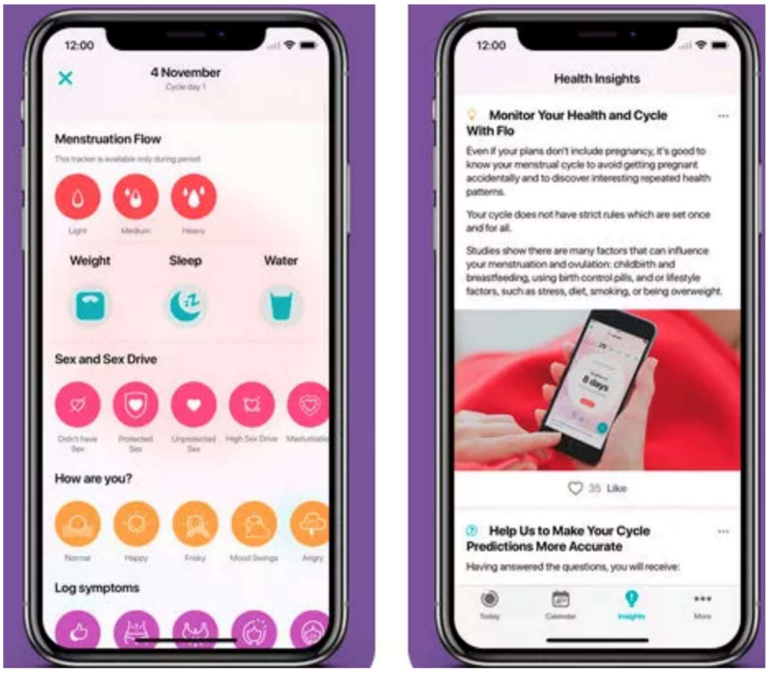
Ovulation and menstrual trackers are part of a growing industry referred to as "Femtech," which is meant to use technology to "improve women's health."[23] They are typically mobile phone applications that operate by asking users to provide various information about their menstrual history and health, and prompt data collection by telling users that the more information they provide, the more accurate their results will be. These trackers, such as Ovia or Flo, not only track when a woman's period occurs, but also the emotional and physical symptoms that occur over the course of their cycle. In order to do so, the apps ask women to input information about their symptoms and activities. Flo, for example, asks users to input the nature of their menstrual flow, sex drive and sexual history, mood, stress level, physical symptoms, and alcohol consumption, among other things. Users are not just asked to provide this information during menstruation, but every day. Although inputting this information is not necessary for the app to

espouses the idea of the "quantified self" as a means to use data to help improve daily life, e.g., by helping with sleep, diet, and other medical problems. *See* Rachael Rettner, *The Quantified Self: How Data-Obsessed Trackers Push Toward Healthier Lives*, HUFFINGTON POST (Apr. 8, 2014), https://www.huffpost.com/entry/quantified-self-health-data-tracking_n_5111958?ncid=fcbklnkushpmg00000043&ir=Science.

[22] For a more extensive list of mobile health apps, and the risks they may pose, *see Healgorithms: Understanding the Potential for Bias in mHealth Apps*, CTR. FOR DEMOCRACY & TECH. (Sept. 13, 2018), https://cdt.org/insight/healgorithms-understanding-the-potential-for-bias-in-mhealth-apps/.

[23] Kate Clark, *It's a New Era for Fertility Tech*, TECHCRUNCH (Feb. 28, 2019), https://techcrunch.com/2019/02/28/its-a-new-era-for-fertility-tech/.

predict users' cycle dates, the app suggests that logging symptoms will improve their cycle predictions.



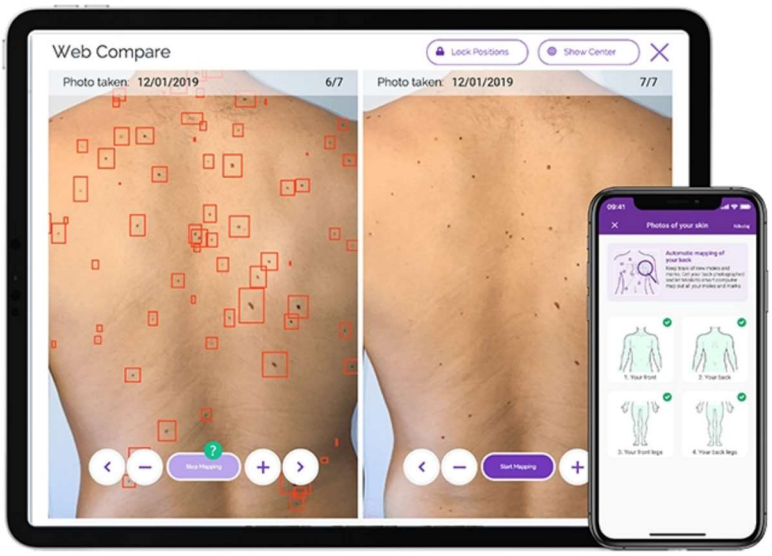
SCREENSHOTS OF FLO[24]

2. Health Diagnostic Apps

Health diagnostic apps prompt users to provide their symptoms and then offer medical solutions based on the information provided. These apps vary significantly from one another in approach and user experience. WebMD's symptom checker, for example, simply asks users for a series of inputs in a standardized format, then displays a list of conditions that match those symptoms. Other health diagnostic apps enable users to submit photos along with other

[24] Erin Migdol, *9 Apps That Can Help People with Chronic Illnesses Track Their Periods*, THE MIGHTY (Feb. 16, 2018) (image excerpted above), https://themighty.com/2018/02/period-tracking-apps-endometriosis-chronic-illness/.

inputs about their symptoms.[25] Still others use artificial intelligence (AI) to simulate the experience of speaking with a doctor. The "health companion" mobile app Ada, for example, asks a series of questions in a back-and-forth exchange that mimics texting with another person.[26] Once the app identifies a potential condition, it allows users to save it to their account and helps them connect with a doctor, pharmacist, or other specialist, if necessary. The Ada app also enables users to specify whether they are trying to obtain a diagnosis for themselves or for a friend. Another health app, Miiskin, helps users keep track of skin spots for early detection of melanoma.[27] Users can upload photos of their skin to the app, which helps them compare any skin changes over time.[28]



SCREENSHOT OF MIISKIN APP[29]

[25] *What We Do and Who We Are*, MIISKIN https://miiskin.com/about/ (last visited Apr. 23, 2019); *Healgorithms: Understanding the Potential for Bias in mHealth Apps*, CTR. FOR DEMOCRACY & TECH. (Sept. 13, 2018), https://cdt.org/insight/healgorithms-understanding-the-potential-for-bias-in-mhealth-apps/.

[26] *About Us*, ADA, https://ada.com/about/ (last visited Apr. 20, 2019).

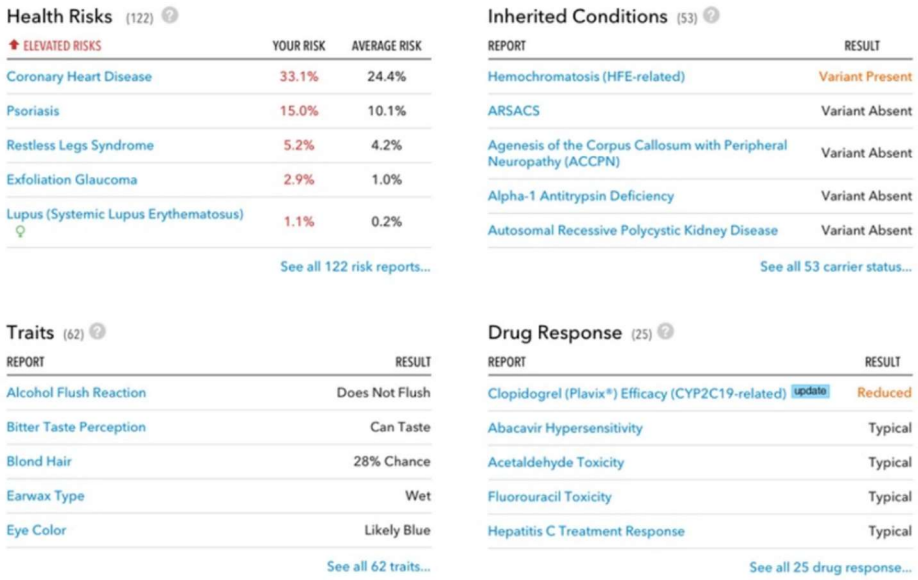
[27] *About Miiskin*, MIISKIN, https://miiskin.com/app/ (last visited Apr. 23, 2019).

[28] *Id.*

[29] *Explore the Miiskin App*, MIISKIN (image excerpted above), https://miiskin.com/app/ (Apr. 23, 2019).

3. Genetic Testing Kits

Direct-to-consumer genetic testing companies like 23andMe have generated a market for at-home DNA testing, promising consumers a means to discover information about their heritage, health, and genetic traits. Typically, users send the company a sample of their DNA and receive a report in a few weeks. These reports can provide a variety of information, including an ethnicity breakdown, potential relatives, predispositions towards certain health conditions, genetic traits, carrier status for various diseases and genetic disorders, and overall wellness information.



Health Risks (122)

ELEVATED RISKS	YOUR RISK	AVERAGE RISK
Coronary Heart Disease	33.1%	24.4%
Psoriasis	15.0%	10.1%
Restless Legs Syndrome	5.2%	4.2%
Exfoliation Glaucoma	2.9%	1.0%
Lupus (Systemic Lupus Erythematosus)	1.1%	0.2%

See all 122 risk reports...

Inherited Conditions (53)

REPORT	RESULT
Hemochromatosis (HFE-related)	Variant Present
ARSACS	Variant Absent
Agenesis of the Corpus Callosum with Peripheral Neuropathy (ACCPN)	Variant Absent
Alpha-1 Antitrypsin Deficiency	Variant Absent
Autosomal Recessive Polycystic Kidney Disease	Variant Absent

See all 53 carrier status...

Traits (62)

REPORT	RESULT
Alcohol Flush Reaction	Does Not Flush
Bitter Taste Perception	Can Taste
Blond Hair	28% Chance
Earwax Type	Wet
Eye Color	Likely Blue

See all 62 traits...

Drug Response (25)

REPORT	RESULT
Clopidogrel (Plavix®) Efficacy (CYP2C19-related) update	Reduced
Abacavir Hypersensitivity	Typical
Acetaldehyde Toxicity	Typical
Fluorouracil Toxicity	Typical
Hepatitis C Treatment Response	Typical

See all 25 drug response...

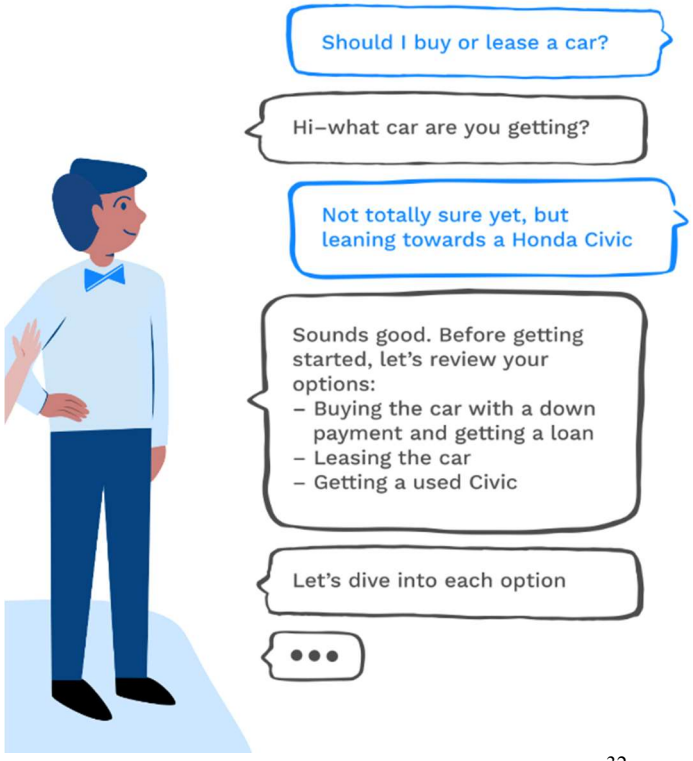
SAMPLE 23ANDME HEALTH REPORT[30]

4. Finance Industry

Outside of the healthcare industry, there are also many products that featurize financial data. Most of these apps are designed to assist with money management, although the types of information they

[30] 23AndMe *Ancestry DNA Test Review: A 10-Minute Deep Dive (2019 Update)*, MY FAMILY DNA TEST (image excerpted above), https://www.myfamilydnatest.com/23andme-review/ (last visited Apr. 25, 2019).

require, and the sophistication of the services they offer, vary significantly. For example, the mobile app Trim claims it will be able to save users money by negotiating down their bills and analyzing their transactions.[31] The Albert app provides investment and savings advice, helps users develop a budget and financial plan, and alerts users when their bills and subscriptions increase. Albert also enables users to engage with it in a text-based format, in order to reach live financial assistants for advice.



SAMPLE DIALOG WITH ALBERT GENIUS[32]

Most of these apps require the user to link their bank account, and some require users to also provide the login information for their various subscriptions.

---

[31] TRIM, https://www.asktrim.com (last visited Apr. 23, 2019).

[32] ALBERT (image excerpted above), https://albert.com/ (last visited Apr. 26, 2019).

These products are marketed in a way that capitalizes on the mentality of the "quantified self" movement—that more information and more revelations make life better. For example, 23andMe's homepage states, "Commit to a healthier you, inspired by your genes—with 125+ genetic reports"[33]; Fitbit's homepage includes the remarks: "Fitbit motivates you to reach your health and fitness goals by tracking your activity, exercise, sleep, weight and more"[34]; Ovia Health, the creator of several fertility and planning apps, states, "We help women and families navigate their most important moments with personalized and data-driven solutions for fertility, pregnancy, and parenting."[35] Finally, Mint's tagline to consumers is, "We help you effortlessly manage your finances in one place."[36] Primary featurization products are thus marketed on the basis that they provide convenience, insight, and savings to the consumer—that they essentially exist to make consumers' lives easier. However, as Part III will discuss, this obscures the privacy and security harms these types of products pose to consumers.

B. Secondary Featurization

Secondary featurization differs from primary featurization in that the product's functionality is not predicated upon user data collection, and, therefore, users may choose not to purchase or use the product on the basis of the value that the data collection process offers.[37] However, as demonstrated with Facebook, users may still engage with that particular feature of the product or acquiesce to that type of data collection as a result of the way the process is marketed.

---

[33] *See Health + Ancestry*, 23ANDME, https://www.23andme.com/?myg=1 (last visited Apr. 24, 2019).

[34] *See* FITBIT, https://www.fitbit.com/home (last visited Apr. 24, 2019).

[35] *See* OVIA HEALTH, https://www.oviahealth.com/ (last visited Apr. 24, 2019).

[36] *See* MINT, https://www.mint.com/ (last visited Apr. 24, 2019).

[37] Tene & Polonetsky, *supra* note 2, at 263-64 (describing quid pro quo featurization in which consumers are likely to be more willing to share information if organizations also provide access to that personal data in formats that can be useful with other third party applications).

Moreover, many of the privacy concerns remain the same as with primary featurization.[38]

Nest's Learning Thermostat is one such example of secondary featurization. Nest's Learning Thermostat primarily functions as a "smart thermometer," meaning that it learns users' energy habits to help regulate temperature in a way that saves them money, and offers the added convenience of being able to be set remotely. Nest also provides users with insight into "their own data trail" by allowing them to see what information it has gleaned about a user's daily routine.[39] While this feature does provide users with valuable information, it is also another way for Nest to collect information about them in a way that is only very loosely connected to its stated purpose.[40] Perhaps this subterfuge makes users more amenable to the fact that these "smart thermometers" are actually using motion sensors to track movements throughout the household.[41]

Another, and perhaps the most quintessential example of secondary featurization, comes from Facebook, the social media website that has been growing and adapting since it was first launched in 2004.[42] One of Facebook's first forays into featurization was the creation of its News Feed, which curates posts generated by users to be displayed in an algorithmically-determined order.[43] Facebook reportedly conceptualized the News Feed as a "personalized list of stories" based on "the latest headlines generated by the activity of your friends and social groups," to combat the chaos and clutter of its Live Feed and provide users with a way to easily see the most relevant updates.[44] Although the change

---

[38] *Infra* Part III.

[39] *See* Tene & Polonetsky, *supra* note 2, at 265.

[40] *Id.*

[41] *See Privacy Statement for Nest Products and Services*, NEST https://nest.com/legal/privacy-statement-for-nest-products-and-services/ (last visited Apr. 29, 2019).

[42] Sarah Phillips, *A Brief History of Facebook*, THE GUARDIAN (July 15, 2007), https://www.theguardian.com/technology/2007/jul/25/media.newmedia.

[43] Josh Constine, *How Facebook News Feed Works*, TECHCRUNCH (Sept. 6, 2016), https://techcrunch.com/2016/09/06/ultimate-guide-to-the-news-feed/.

[44] Samantha Murphy, *The Evolution of Facebook News Feed*, MASHABLE (Mar. 12, 2013), https://mashable.com/2013/03/12/facebook-news-feed-evolution/#IoSYn_ZKLPq0.

initially incurred protests and privacy concerns, it quickly became an integral part of Facebook's interface.[45]

Nearly ten years later, Facebook revealed its data scientists had been manipulating the News Feeds of hundreds of thousands of users in order to conduct a psychological study assessing "how emotions can be spread on social media."[46] They did this by randomly selecting users and changing the number of positive or negative posts they saw.[47] Notably, an analyst commented that "Facebook didn't do anything illegal, but they didn't do right by their customers."[48] Although Facebook ended that experiment with an apology, they subsequently manipulated News Feeds in another way: by removing professional news posts.[49] That move was also met with significant criticism, including commentary that Facebook was "increasing fake news and misinformation on the platform."[50]

Facebook's News Feed is just one of many features offered to its users that enabled the company to obtain more information about individuals, and to propel data usages not initially intended nor made publicly clear. In 2010, Facebook also rolled out a photo-tagging feature that suggested the names of individuals in each photo, purportedly to save time when uploading photos.[51] According to some advocacy groups, the company did not adequately explain to users, however, that by providing identifying information—the

---

[45] Mercedes Bunz, *Facebook Users Protest Over News Feed*, THE GUARDIAN (Oct. 27, 2009), https://www.theguardian.com/media/pda/2009/oct/27/new-facebook-newsfeed-protest.

[46] Vindu Goel, *Facebook Tinkers with Users' Emotions in News Feed Experiment, Stirring Outcry*, N.Y. TIMES (June 29, 2014), https://www.nytimes.com/2014/06/30/technology/facebook-tinkers-with-users-emotions-in-news-feed-experiment-stirring-outcry.html.

[47] *Id.*

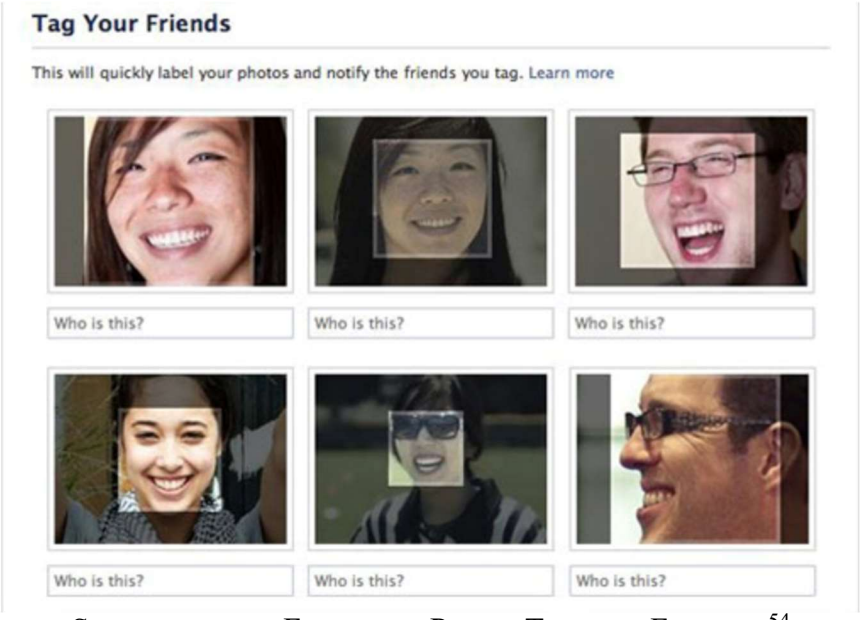
[48] *Id.*

[49] Alex Hern, *Facebook Moving Non-Promoted Posts Out of News Feed in Trial*, THE GUARDIAN (Oct. 23, 2017), https://www.theguardian.com/technology/2017/oct/23/facebook-non-promoted-posts-news-feed-new-trial-publishers.

[50] Julia Carrie Wong, *Facebook Ending News Feed Experiment Condemned as 'Orwellian'*, THE GUARDIAN (Mar. 1, 2018), https://www.theguardian.com/technology/2018/mar/01/facebook-news-feed-experiment-media-posts.

[51] Murphy, *supra* note 44.

"tag"—to their photos, users were actually honing the company's facial recognition technology.[52] Meanwhile, as each new feature was introduced, all in the name of the consumer, Facebook slowly began to pull back on the privacy protections it offered.[53]



SCREENSHOT OF FACEBOOK PHOTO TAGGING FEATURE[54]

With featurization, the collection and use of data often begins as a way to add value for consumers. Yet, there remains no protection against repurposing that data, even if it happens years later. Moreover, as discussed in the following part, users often lack

---

[52] Complaint In re Facebook, Inc. and Facial Recognition, (filed Apr. 6, 2018), https://www.epic.org/privacy/facebook/FTC-Facebook-FR-Complaint-04062018.pdf.

[53] Kurt Opsahl, *Facebook's Eroding Privacy Policy: A Timeline*, ELEC. FRONTIER FOUND. (Apr. 28, 2010), https://www.eff.org/deeplinks/2010/04/facebook-timeline.

[54] Ben Parr, *Facebook brings facial recognition to photo tagging*, CNN (Dec. 16, 2010) (image excerpted above), http://www.cnn.com/2010/TECH/social.media/12/16/facebook.facial.recognition.mashable/index.html.

adequate remedies if they are unhappy with the privacy concerns that manifest later.

II. EXISTING PRIVACY AND SECURITY PROTECTIONS

Currently, the United States does not have a comprehensive federal law governing privacy. Rather, privacy laws and regulations in the United States are broken up into two main branches.[55] First are the several sectoral privacy laws that govern more sensitive areas of information including healthcare, finance credit information, and information relating to children.[56] The second branch comes from the Federal Trade Commission's enforcement authority under Section 5 of the Federal Trade Commission Act ("FTCA").[57] Certain other laws, like California's recently passed California Consumer Privacy Act ("CCPA") and the EU's General Data Protection Regulation ("GDPR"), also apply to many U.S. companies.[58] Each of these laws is discussed in more detail below.

A. Sectoral U.S. Privacy Laws

Sectoral privacy laws are limited in scope. They only protect certain types of information, under certain circumstances. The Gramm-Leach-Bliley Act ("GLBA"), for example, protects financial information, but only applies to "financial institutions" that engage in activities such as lending or exchanging money, providing loans, or collecting debts.[59] Similarly, The Health Insurance

---

[55] *See* Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

[56] Children's Online Privacy Protection Act, 15 U.S.C.A. § 6502 (West 2019); Health Insurance Portability and Accountability Act, 45 C.F.R. § 164.105 (2019); Gramm-Leach-Bliley Act, 15 U.S.C.A. § 6801 (West 2019); Fair Credit Reporting Act, 15 U.S.C.A. § 1681 (2019).

[57] 15 U.S.C. § 45(a)(1) (2006).

[58] California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (West 2019) (effective Jan. 1, 2020); Council Regulation 2016/679, 2016 O.J. (L 119) 1, 5 (EU) [hereinafter GDPR].

[59] 16 C.F.R. § 313.1 (2019); *How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, FTC (July 2002),

Portability and Accountability Act ("HIPAA") only applies to "covered entities," which include healthcare providers such as doctors and pharmacists, health plans, health clearinghouses, and the business associates of these entities.[60] Consequently, companies that provide at-home DNA testing kits would not be regulated by HIPAA, nor would most mobile medical apps. As a result, even though these apps may collect information that is equally as sensitive as the type of information individuals may share with their doctor, these companies are not subject to heightened regulations governing how they may use or share that data.[61]

B. FTC Enforcement

The Federal Trade Commission ("FTC") is the primary regulator of U.S. privacy law.[62] Although the FTC's enforcement authority is broader and could extend to the companies that create and sell products that featurize data, it is limited in other respects. Rather than regulate affirmative privacy requirements under Section 5 of the FTCA, the FTC regulates against "unfair or deceptive acts or practices" affecting commerce.[63] In that sense, rather than propagate general privacy requirements, the FTC must look at business practices individually to determine whether they are unfair or deceptive. While this enables the FTC to respond to new threats to data privacy and security as they emerge, those concepts are difficult to define in the context of featurization.

The FTC primarily regulates privacy violations under the "deceptive" prong of its authority precisely because unfairness is a

---

https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm#whois.

[60] *See* 45 C.F.R. § 160.103 (2014).

[61] *See, e.g.*, Drabiak, *supra* note 10 at 146.

[62] *See* Press Release, FTC, FTC Releases 2018 Privacy and Data Security Update, (Mar. 15, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-releases-2018-privacy-data-security-update.

[63] Robert Gellman, *Can Consumers Trust the FTC to Protect Their Privacy?*, ACLU (Oct. 25, 2016), https://www.aclu.org/blog/privacy-technology/internet-privacy/can-consumers-trust-ftc-protect-their-privacy.

slippery term.[64] But, the harms of featurization may not be considered a "deceptive practice" because this usually requires that a company violated an explicit promise it made, such as in its privacy policy.[65] In most cases of harm posed by featurization, the privacy policy enumerates the ways in which individuals' data might be used; it may just not be facially apparent. In addition, companies may write vague policies to avoid FTC scrutiny or modify their policies as they discover more uses for the data.[66] Because of this, there may be "little the FTC can do."[67]

Moreover, the FTC's primary way of penalizing a company that has engaged in an unfair or deceptive practice is to issue a consent decree.[68] This typically requires the offending company to implement certain privacy and security programs and subjects them to twenty years of FTC oversight.[69] However, for bigger and more profitable companies, the FTC's bark may still be worse than its bite.[70] Facebook, for example, has been subject to a consent decree for nearly ten years, though recent news about the company suggests that the decree has had little impact.[71] The FTC has developed important privacy requirements over time through its enforcement authority.[72] However, without more affirmative enforcement authority, the FTC alone will not be able to mitigate these concerns.

---

[64] Joseph Jerome, *Can FTC Consent Orders Effectively Police Privacy?*, INT'L. ASS'N OF PRIVACY PROF. (Nov. 27, 2018), https://iapp.org/news/a/can-ftc-consent-orders-police-privacy/ (a "showing of injury [is] not easily met in privacy disputes").

[65] Gellman, *supra* note 63.

[66] *Id.*

[67] *Id.*

[68] *See* Jerome, *supra* note 64.

[69] *Id.*

[70] *Id.; see also* Nitasha Tiku, *Why Facebook's 2011 Promises Haven't Protected Users*, WIRED (Apr. 11, 2018), https://www.wired.com/story/why-facebooks-2011-promises-havent-protected-users/.

[71] *See* Jerome, *supra* note 64, ("But as the FTC's oversight of Facebook reaches its midpoint, there is growing evidence that these orders simply create box-checking exercises without protecting anyone's privacy.").

[72] *See, e.g.*, Press Release, FTC, FTC's $5 billion Facebook settlement: Record-breaking and history-making (July 24, 2019) https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history.

Increasingly, the FTC is using its "unfairness" authority to regulate data security measures.[73] When addressing unfairness, the FTC considers three factors: (1) whether the practice, even if not unlawful, offends public policy; (2) whether it is immoral, unethical, oppressive, or unscrupulous; and (3) whether it causes substantial injury to consumers.[74] For data security practices, this means the FTC requires that companies engage in encryption protocols compatible with industry standards and factor in the risk of security breaches when making decisions about how to store their users' data.[75] However, this may not be adequate to protect against data breaches of featurized data—both because this type of data, which is provided directly by the user, may be extraordinarily sensitive, and because the FTC's practice of penalizing companies after the harm has occurred may not be sufficient to protect against future breaches by developing standards to protect against future harms as technology advances.[76]

C. California Consumer Privacy Act

The CCPA offers new privacy protections for California residents and imposes additional requirements on larger companies that collect users' personal information.[77] In particular, the CCPA's purpose limitation requirement and rights of access and deletion all offer some protections for data collected through featurization.[78] However, the CCPA may not be sufficient to protect against all types of harms caused by featurization.

---

[73] *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 243 (3d Cir. 2015).

[74] *Id*.

[75] *See* Patricia Bailin, *Study: What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices*, INT'L. ASSOC. OF PRIVACY PROF.. (Sept. 19, 2014), https://iapp.org/media/pdf/resource_center/FTC-WhitePaper_V4.pdf.

[76] *See, e.g.*, Adam Mazmanian, *Senate Bill Would Give FTC New Data Breach Authority*, FED. COMPUTER WK. (Jan. 10, 2018), https://fcw.com/articles/2018/01/10/ftc-data-breach-mazmanian.aspx.

[77] California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.100 (West 2019) (effective Jan. 1, 2020).

[78] *Id.*

The CCPA requires companies to provide individuals with information regarding the categories of personal information a company collects, as well as the purposes for which that information will be used.[79] In addition, individuals may request information on the categories of personal information that is collected and the company's purposes for collecting or selling it.[80] Such disclosures could help individuals understand how their data is being used if the information is provided to them in an easily understandable format. Nonetheless, this right to request information does not prevent the types of adverse uses featurization implicates and would only require disclosure after the fact.

The CCPA also imposes certain purpose limitation requirements.[81] Under the law, businesses may not use collected information "for additional purposes without providing the consumer with notice and consent."[82] The CCPA also prohibits companies from collecting, selling, or using personal information "except as necessary to perform the business purpose."[83] Additionally, in the event of a merger under the CCPA, covered companies must provide users with the right to opt out if the "third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection."[84] However, these protections may be inadequate against all the harms caused by featurization. Unless notice is displayed prominently and consent is obtained in a way that is meaningful, it is unclear whether this notice and consent requirement adds anything meaningful to the existing

---

[79] *Id.*

[80] *Privacy Framework Comparisons*, CTR. FOR DEMOCRACY & TECH., 3 (Dec. 2018), https://cdt.org/files/2018/12/2018-12-12-CDT-CCPA-GDPR-Chart-FINAL.pdf.

[81] CAL. CIV. CODE § 1798.100.

[82] *Id.* § 1798.100(b).

[83] CAL. CIV. CODE § 1798.140(t)(ii).

[84] *See* DATAGUIDANCE, *Comparing Privacy Laws: GDPR v. CCPA*, FUTURE OF PRIVACY FORUM, 5 (2018), https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf.

privacy framework.[85] Moreover, companies may choose to only afford certain rights—like the opt-in mechanism—to California residents, which they are legally entitled to do under the law.[86] In addition, the CCPA excludes aggregate and deidentified data, as well as processing done on data that is "publicly available," which may undercut some of the protections it affords.[87]

D. General Data Protection Regulation

The GDPR grants certain affirmative privacy rights to individuals and is similar to the CCPA in several respects. The GDPR provides data access rights like the CCPA, and it also imposes strict purpose limitations and data minimization requirements on data controllers and processors.[88] Under the GDPR, data may only be collected for a specified purpose and cannot be "further processed in a manner that is incompatible with those purposes."[89] This purpose specification analysis must be done via case-by-case analysis to determine whether further processing is compatible by examining, among other things, the context of the data collection, the relationship between the purposes for data collection and the purposes for further processing, the nature of the data, and the impact further processing may have on the data subjects.[90] Moreover, personal data cannot be stored for longer than "is necessary for the purposes for which the personal data are processed."[91] In addition, the Article 29 Working Party, a recently decommissioned European data protection advisory board, clarified that these purposes must achieve a certain level of specificity, and that information related to privacy should be delivered in a multi-

---

[85] *See, e.g.*, SOLON BAROCAS & HELEN NISSENBAUM, ON NOTICE: THE TROUBLE WITH NOTICE AND CONSENT (2009), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567409.

[86] *See* CAL. CIV. CODE § 1798.140(g) ("'Consumer' means a natural person who is a California resident, as defined in . . . the California Code of Regulations[.]")

[87] *See* CAL. CIV. CODE § 1798.145(a)(5).

[88] GDPR art. 24-43.

[89] GDPR, art. 5.

[90] DATAGUIDANCE *supra* note 84.

[91] GDPR, art. 5(1)(b).

layered notice to consumers to ensure they are accessible and easily readable.[92]

Although these provisions appear to offer some meaningful protections, the nature of featurization may still subvert them—particularly in instances where adverse uses are enumerated in the Terms of Service from the product's inception, and the benefits that the data can provide require that it be stored for a long period of time. Returning to the genetic-testing kit example, individuals may want their DNA data to be stored for continued access; or, they may have granted research rights to these companies, thus enabling the companies to keep data for several years in order to serve that purpose. However, throughout that time, the company could still use that data and engage in practices that are adverse to the individual's interest if that type of use was included in the fine print.[93]

It is also worth noting that the GDPR has only recently been enacted and has only been in effect since May 2018. Accordingly, it may take more time before the contours of these provisions become clear.

III. CONCERNS UNDER EXISTING LAW

Many of the harms posed by featurized products stem from the increase in quantity and sensitivity of the information they are able to elicit from consumers. These products, and the value they purport to offer, make consumers more willing to input and interact with their data in ways that are more revealing than ever before. It is this willingness to increase one's data trail, for particularly sensitive information, from which additional harms flow. Existing law is ill-equipped to address the issues that featurization presents. The patchwork of laws that govern privacy in the United States

---

[92] Council Directive 95/46/EC, art. 29, Data Protection Working Party (Nov. 2017), at 6-8.

[93] *See, e.g.*, Erin Brodwin, *DNA Testing Company 23andMe has Signed a $300 Million Deal with a Drug Giant — Here's How to Delete Your Data if that Freaks You Out*, BUS. INSIDER (July 25, 2018), https://markets.businessinsider.com/news/stocks/dna-testing-delete-your-data-23andme-ancestry-2018-7-1027400770; Piotr Foitzik, *How to Apply the GDPR Data Minimization Principle to Online Sales*, INT'L ASS'N OF PRIVACY PROF'L. (Feb. 26, 2019), https://iapp.org/news/a/how-to-apply-the-gdpr-data-minimization-principle-to-online-sales/.

predominantly follow a notice and consent model, which may be insufficient to provide adequate protections in the context of featurization—particularly where users are inputting data themselves, rather than passively having data collected about them. Moreover, most U.S. laws that govern sensitive personal information, like health or financial information, would not apply to companies that engage in featurization. Other mechanisms for enforcement of privacy protections, like the FTC's Section 5 authority or industry self-regulation, may also fall short. Similarly, California's new CCPA and Europe's GDPR offer more affirmative privacy protections, but also may not go far enough to protect against the types of harms that featurization presents.

Featurized products elicit sharing of personal information that is viewed as intrinsically private. This sharing facilitates new uses for data that companies otherwise would not have access to. Most people, for instance, probably would not approve of a company maintaining a proprietary interest in their DNA and then selling it to pharmaceutical companies. Nonetheless, that is exactly how at-home genetic testing companies like 23andMe operate, and millions of users provide them with their data every day.[94] The reason, of course, is likely that they were interested in learning more about their ancestry or health background and found companies whose stated purpose was to do exactly that, without considering what might happen to their data afterwards.[95]

In addition to encouraging data sharing, featurized products may increase an individual's data trail by combining or selling their data to third parties. An individual's data from various accounts can be combined in the event of a merger, or a single company may collect data on its users in different ways, and subsequently combine them to create more holistic profiles of each one.[96] Returning to at-home genetic testing as an example, consumer genetics companies like 23andMe have generated a market for at-home DNA testing, promising consumers a means to discover information about their

[94] Drabiak, *supra* note 10, at 147 (81.5% of consumers further stated they would get genomic testing done if they could afford to).

[95] *See, e.g.*, Opsahl, *supra* note 53.

[96] *See, e.g.*, Johnston, *supra* note 18.

heritage, health, and traits.[97] While the marketing suggests these companies are targeted towards the direct-to-consumer market and create products solely for the purpose of allowing individuals to discover more about themselves, the truth is that 23andMe's intended market was never just consumers.[98] Rather, genomics companies have collected a significant amount of information, which "makes them appealing to a number of additional parties, including data brokers, the pharmaceutical industry, employers, health insurers, and law enforcement."[99]

In both instances, a user's data profile is expanded in ways that were likely unforeseeable to them and could then be used for purposes that are adverse to their interests, or make them even more vulnerable in the event of a data breach.[100] This increase in an individual's data trail, coupled with an absence of clear regulation addressing featurization, has led to three main harms: (1) increased vulnerability to data breaches, (2) the expansion in scope of permissible surveillance by law enforcement, and (3) discrimination resulting in economic loss. It is worth noting that these harms are also much more likely to be felt acutely by marginalized communities, particularly low-income communities and communities of color.

A. Increased Vulnerability to Data Breaches

An increased data trail combined with additional data sharing makes individuals vulnerable to data breaches, simply because their data exists in more places, and in more sensitive and revealing ways.[101] As consumers come to rely on featurized products for

---

[97] 23ANDME *supra* note 3.

[98] Molteni, *supra* note 7.

[99] Drabiak, *supra* note 10, at 149.

[100] Max Eddy, *Turning a Nest Smart Thermostat into a Data-Stealing Spy in 15 Seconds*, PC MAG: SECURITYWATCH (Aug. 7, 2014), https://securitywatch.pcmag.com/hacking/326209-turning-a-nest-smart-thermostat-into-a-data-stealing-spy-in-15-seconds.

[101] *See, e.g.*, Daniel Zwerdling & G.W. Schulz, *Your Digital Trail, and How It Can Be Used Against You*, NPR (Sept. 30, 2013), https://www.npr.org/sections/alltechconsidered/2013/09/30/226835934/your-digital-trail-and-how-it-can-be-used-against-you.

multiple purposes and across various industries, it likely increases their "attack surface"—that is, the number of potential avenues for their sensitive information to be exposed or exploited.[102] This is particularly true as individuals use these types of products across several different sectors without assessing the compound effects this might have on the protection of their data overall.

Moreover, it makes individuals vulnerable to more harmful types of data breaches. Nest data, for example, would be able to tell adversaries when an individual is out of the home or on vacation—information that could be used "for future digital attacks, or simply for burglary."[103] DNA data is also enticing to potential hackers because of its uniquely identifying nature. In several recent instances hackers broke into DNA databases and held sensitive personal data for ransom.[104] Hackers could also sell this information to data brokers or other interested parties who could then use that information to discriminate against or target individuals in a variety of contexts.[105] While these concerns are in a far-off and perhaps uncertain future, they still highlight how certain types of data can be much more harmful if leaked. As some experts have pointed out, you can change your credit card number, but you can never change your DNA.[106]

While no data is guaranteed to be secure, existing laws are not yet sufficient to ensure this data is required to be kept as cryptographically safe as possible. There have been numerous instances of featurized products containing easily exploitable

---

[102] *See* Tim Woods, *5 Ways to Reduce Your Attack Surface*, SECURITY MAGAZINE (Aug. 2, 2018), https://www.securitymagazine.com/articles/89283-ways-to-reduce-your-attack-surface; Lily Hay Newman, *Hacker Lexicon: What Is an Attack Surface*, WIRED (Mar. 12, 2017), https://www.wired.com/2017/03/hacker-lexicon-attack-surface/.

[103] Eddy, *supra* note 100.

[104] *See* Zeljka Zorz, *US Hospital Paid $55,000 Ransom to Hackers Despite Having Backups*, HELPNET SECURITY (Jan. 17, 2018), https://www.helpnetsecurity.com/2018/01/17/hospital-ransomware/; Angela Chen, *Why a DNA Data Breach is Much Worse than a Credit Card Leak*, THE VERGE (June 6, 2018), https://www.theverge.com/2018/6/6/17435166/myheritage-dna-breach-genetic-privacy-bioethics.

[105] Chen, *supra* note 104.

[106] *Id*.

glitches, or even times when that data was actually hacked.[107] Because the companies that create many of these featurized products are not required to comply with strict regulations, it is up to these companies themselves to maintain stringent enough standards to prevent data breaches.[108] This has often not worked out.[109] It was recently reported, for example, that a fertility planner app contained a glitch that would have allowed "someone with no hacking skills at all" to access highly sensitive information about the women who use the app.[110] While these apps do not necessarily present an above average risk of data breach compared to others on the market, it is the sensitivity of the information they collect that makes data breaches of this kind to be a particularly serious harm. In the case of fertility apps, these companies collect several strands of sensitive information, including the user's history of abortions, moods, medications, and smoking or drinking habits.[111] But, because sectoral privacy laws like HIPAA do not apply to these types of companies, they have no heightened incentive to protect this information.

B. Expanding the Scope of Permissible Surveillance

Featurization vastly expands the types of information accessible to law enforcement without a warrant. Traditional privacy protections granted under the Fourth Amendment do not apply to information voluntarily shared with third parties.[112] Because

---

[107] *See, e.g.*, GRANT HERNANDEZ ET AL. SMART NEST THERMOSTAT: A SMART SPY IN YOUR HOME (2014), https://www.blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home-WP.pdf; Zach Whittaker, *DNA Testing Startup Veritas Genetics Confirms Data Breach*, TechCrunch (Nov. 7, 2019), https://techcrunch.com/2019/11/07/veritas-genetics-data-breach/; Jerry Beilinson, *Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds*, CONSUMER REPORTS (July 28, 2016), https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats/.

[108] *See, e.g.*, Beilinson, *supra* note 107.

[109] *Id.*

[110] *Id.*

[111] Burke, *supra* note 8; Beilinson, *supra* note 107.

[112] The Supreme Court's recent decision in *Carpenter v. United States* complicates the third party doctrine slightly by introducing additional analysis

featurized products are predicated on individuals intentionally providing what is often highly sensitive and personal information, it could mean they are inadvertently enabling law enforcement to access this information.

There are considerable risks associated with DNA data. The popularity of at-home genetic testing has created databases containing millions of people's DNA, which law enforcement has already accessed without a warrant and likely will continue to do.[113] Moreover, when individuals submit their DNA to a company, their family members are at risk of identification too. Through a process called familial matching, police are able to compare DNA from a crime scene to DNA in databases to search for partial matches, which potentially indicates the suspect is a relative of the match.[114] In a recent high-profile case, police were finally able to catch Joseph James DeAngelo, the Golden State Killer, in 2018 by creating a fake profile on GEDMatch, a public DNA database and uploading DNA collected from previous crime scenes to search for a matches.[115] They were able to identify DeAngelo after their sample matched the DNA of DeAngelo's relatives, who were on the site.[116]

---

that may be factored in. However, currently, it is unclear how this will play out in contexts beyond the one at issue in that case (CSLI data). *See Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018) ("In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."); *see also*, Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J.L. & TECH. 352, 361-66 (2019).

[113] Press Release, U.S. Dep't of Justice, Department of Justice Announces Interim Policy on Emerging Methods to Generate Leads for Unsolved Violent Crimes (Sept. 24, 2019), https://www.justice.gov/opa/pr/department-justice-announces-interim-policy-emerging-method-generate-leads-unsolved-violent; Megan Molteni, *The Future of Crime-Fighting is Family Tree Forensics*, WIRED (Dec. 26, 2018), https://www.wired.com/story/the-future-of-crime-fighting-is-family-tree-forensics/.

[114] *See* Molteni, *supra* note 113.

[115] *See* Rachel Becker, *Golden State Killer Suspect was Tracked Through Geneology Website GEDMatch*, THE VERGE (Apr. 26, 2018), https://www.theverge.com/2018/4/26/17288532/golden-state-killer-east-area-rapist-genealogy-websites-dna-genetic-investigation.

[116] *Id.*

DNA is not the only type of sensitive information that law enforcement may now have greater access to. Law enforcement has already requested data from wearables, like a Fitbit, to assist in ongoing investigations and could foreseeably demand biometric data or other sensitive information be shared with them as well.[117] In instances where law enforcement may access an entire database of information at a time, it could enable systems of mass surveillance that are ripe for abuse.[118] Under existing law, there are few protections to protect against this kind of expansion in law enforcement's power.[119]

C. Discrimination and Economic Loss

Use of featurized products may also lead to discrimination against and economic loss for certain individuals. Insurance companies, employers, and other third parties who may access this data could use it to perform predictive analytics in ways that discriminate against certain individuals, or otherwise cause harm. For example, DNA sequencing may one day be used to predict individuals' "susceptibility to adverse health conditions and development of disease."[120] Insurance companies may increase their premiums for individuals who are genetically more likely to acquire a certain disease. Loan companies may deny loans if data predicts that a potential borrower could get a disease and die before they can

---

[117] *See, e.g.*, Christine Hauser, *Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing*, N.Y. TIMES (Oct. 3, 2018), https://www.nytimes.com/2018/10/03/us/fitbit-murder-arrest.html; Amanda Watts, *Cops Use Murdered Woman's Fitbit to Charge her Husband*, CNN (Apr. 26, 2017), https://www.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html; Jay Stanley, *Local Police Using and Abusing DNA and Other Biometric Technologies*, ACLU (Sept. 13, 2016), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/local-police-using-and-abusing-dna-and-other.

[118] Bryson Masse, *What's the Worst that Could Happen with Huge Databases of Biometric Data?*, GIZMODO (Sept. 11, 2017), https://gizmodo.com/what-s-the-worst-that-could-happen-with-huge-databases-1802696698.

[119] *See* Tom Simonite, *Few Rules Govern Police Use of Facial-Recognition Technology*, WIRED (May 22, 2018), https://www.wired.com/story/few-rules-govern-police-use-of-facial-recognition-technology/.

[120] Drabiak, *supra* note 10, at 146.

pay their debt back. Credit scoring companies, too, may be repurposing this type of data in ways that may cause future financial harms to consumers.[121]

In addition, while the majority of featurized products in use currently are obtained in a personal capacity for personal use, the companies that create these products are increasingly partnering with employers and insurance companies in order to create mechanisms for monitoring employees or subscribers.[122] The pregnancy and menstrual tracker Ovia, for example, recently came under fire for partnering with employers and sharing data with employers relating to their employees in an aggregate format.[123] In the case of Ovia, employees must opt in before their data can be shared with employers, even in aggregate format.[124] However, many are concerned that these companies are targeting individuals who are in an incredibly vulnerable position, and consumers may not realize exactly what they are giving away.[125] In addition, employers may entice their employees to provide this information through monetary incentives or other rewards. Activision Blizzard, for example, offered its female employees one dollar a day to opt into the employer version of Ovia.[126] As one woman put it, "that's money for diapers and bottles."[127] But, without more limitations on the collection and use of this data, employers may be able to use this information in largely invisible ways that are harmful to their employees. Although existing discrimination laws protect against wrongful terminations on the basis of pregnancy, for example, that

---

[121] Tatiana Dias & Igor Natusch, *They Are Stalking You to Calculate Your Credit Score*, CHUPADADOS, https://chupadados.codingrights.org/en/they-are-stalking-you-to-calculate-your-score/ (last visited Apr. 29, 2019).

[122] *See, e.g.*, Drew Harwell, *Is Your Pregnancy App Sharing Your Intimate Data with Your Boss?*, WASH. POST (Apr. 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/?utm_term=.ff0399d9ca1c.

[123] *Id*.

[124] *Ovia Health Privacy Policy*, OVIA, https://www.ovuline.com/dynamic-privacy (last visited Apr. 9, 2019).

[125] Harwell, *supra* note 122.

[126] *Id*.

[127] *Id.*

alone may not be sufficient to deter the wrongful conduct of all potentially implicated employers.

Finally, in the adverse data-sharing context, data may be sold to data brokers or other for-profit third parties. This can lead to a number of subsequent issues, including placing people in high-risk classifications, and marketing to them in predatory ways.[128] These companies can already tell "if you've just gone through a break-up, if you're pregnant or trying to lose weight, whether you're an extrovert, what medicine you take, where you've been, and even how you swipe and tap on your phone."[129] Combining this information with featurized product data may allow data brokers to infer even more about individuals, including highly sensitive information.

D. Impact on Vulnerable Communities

These harms may be most acutely felt by vulnerable populations, such as low-income communities. Individuals with fewer resources may increasingly rely on these products to fill in areas of life that are otherwise unaffordable.[130] Because many featurized products, like diagnostic medical apps or AI-enhanced financial assistant apps, offer services that would otherwise be expensive, it is more likely that these communities would come to rely on them more. These vulnerable populations may use featurized apps as substitutes for doctors or other established institutions. Thus, the risks posed are enhanced for these populations, particularly in these instances.[131]

Because federal regulations have yet to catch up to some of these technologies, the consequences for these individuals could be severe. For example, featurized applications are not legally required

---

[128] Yael Grauer, *What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?*, VICE (Mar. 27, 2018), https://motherboard.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection.

[129] Steven Melendez & Alex Pasternack, *Here Are the Data Brokers Quietly Buying and Selling Your Personal Information*, FAST COMPANY (Mar. 2, 2019), https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information.

[130] *See, e.g.*, CENTER FOR DEMOCRACY & TECHNOLOGY *supra* note 25.

[131] *Id*.

to be accurate.[132] Pregnancy tracker apps have recently come under fire for being inaccurate,[133] and, diagnostic apps, although they may caveat that they are not a substitute for medical professionals, could also incorrectly diagnose individuals in ways that deter them from getting medical treatment or cause them to seek the wrong type of treatment.[134] This is especially true considering that artificial intelligence enhanced applications are already notorious for their bias against people of color and women.[135]

IV. RECOMMENDATIONS

A. Create Statutory Limitations on the Third-Party Doctrine

Federal law needs to evolve to protect featurized data above the Fourth Amendment baseline. Although the Supreme Court in *Carpenter* held that the Fourth Amendment protects private cell-phone location data from warrantless searches, as of now, it is unclear whether that analysis would apply to featurization.[136] Crafting a warrant requirement for highly personal and sensitive information like the DNA or biometric identifiers held in either public or private databases would help ensure that this information is not used adversely for law enforcement purposes. Some states have already enacted laws for these purposes. For example, California requires law enforcement to obtain a warrant before gaining access to data from digital voice assistants.[137] However,

---

[132] Although inaccuracy could incur an unfair and deceptive act and practices claim by the FTC, this may not be sufficient to deter the practice universally.

[133] Alexandra Sifferlin, *Why Your Period Tracker is Wrong*, TIME (June 8, 2016), http://time.com/4361855/period-tracker-fertility-tracker-app/.

[134] CENTER FOR DEMOCRACY & TECHNOLOGY, *supra* note 25.

[135] Joy Buolamwini, *Artificial Intelligence Has a Problem with Gender and Racial Bias. Here's How to Solve It*, TIME (Feb. 7, 2019), http://time.com/5520558/artificial-intelligence-racial-gender-bias/.

[136] *See Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018).

[137] *See* Geoffrey A. Fowler, *Alexa Has Been Eavesdropping on You this Whole Time*, WASH. POST (May 6, 2019), https://www.washingtonpost.com/pb/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/?nid=menu_nav_accessibilityforscreenreader&outputType=accessibility&utm_term=.1f327d41ca84.

merely requiring a warrant for this type of data is not sufficient to protect users' personal information. Those on the receiving end must also challenge overbroad warrants or those that are not sufficiently particularized.[138]

B. Increase Oversight into Products in Sensitive Industries

Federal law must adapt to the rise of featurization and provide greater protections for the information collected by these products, particularly in sensitive areas like health and finance. This can be accomplished in several ways, including amending sectoral privacy laws like HIPAA and the GLBA to cover these types of products, or crafting new laws specifically targeting featurization. Regardless, these laws must include provisions to ensure security, accuracy, and fairness.

1. Security

Under existing law, there is only a patchwork of security requirements for individuals' data. HIPAA, for example, includes an affirmative cybersecurity requirement for personal information held by covered entities, and, currently, the FTC is in the notice-and-comment phase of amending the GLBA to include more detailed and stringent security measures regarding financial information.[139] These two laws, however, would likely not apply to the majority of featurized products in the health and finance spaces. The FTC's Section 5 authority governs cybersecurity requirements for most other players in industry. However, under the FTC's unfair and deceptive practice enforcement alone, it is difficult to ensure that all companies are maintaining sufficient cybersecurity

---

[138] *See, e.g.*, Cassie Martin, *Why a Warrant to Search GEDMatch's Genetic Data Has Sparked Privacy Concerns*, SCIENCENEWS (Nov. 12, 2019), sciencenews.org/article/why-warrant-search-gedmatch-genetic-data-has-sparked-privacy-concerns; *How to Challenge Digital Device Searches*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/criminaldefender/digital-device-searches/how-to-challenge#lack_of_specificity. (last accessed Apr. 27, 2019).

[139] P.L. No. 104-191, 110 Stat. 1938 (1996); 16 U.S.C. § 6803(f).

standards, and, moreover, to identify those who are not, before individuals' data is compromised.

A federal law that creates a safe harbor or certification for companies that voluntarily enact more stringent cybersecurity requirements, similar to the Cyber Shield Bill that Senator Markey introduced in 2017, could provide the requisite incentive to ensure individuals' data is safer, without being overly-burdensome to small companies who may find compliance too onerous.[140] If that certification were displayed prominently, users would be able to make better-informed choices about each product they use.

2. Fairness

Featurized data in the health and finance sectors must be guarded from misuse. Accordingly, the law should prohibit this data from being used in ways that are adverse to the individuals' interest. For example, federal law should unilaterally prohibit featurized data—like DNA data collected through at-home genetic testing kits—from being sold to insurance companies or employers unless pseudonymized in a way that prohibits re-identification of specific consumers. Moreover, in instances where the data would be sold to third parties without aggregation or pseudonymization, the company must acquire the individuals' express consent.

3. Accuracy

Featurized products must also be regulated for accuracy, particularly when they may act as a substitute for in-person services, such as financial assistance or diagnostic medical applications. Moreover, because these types of products may impact vulnerable populations more severely, any new federal law should be required to conduct impact assessments on how, in particular, they perform within regard to vulnerable populations.

[140] Cyber Shield Act of 2017, S. 2020, 115th Cong. § 1 (2017).

CONCLUSION

Featurization can benefit consumers by promoting greater awareness of health, finance, and energy habits. However, the data collected by this process is ripe for abuse—both by law enforcement and by private companies. The companies that collect this data can not only gather both a greater amount and more sensitive information about individuals, but also profit off of this practice in ways that pose significant privacy risks to users. There must be stronger privacy protections enacted in order to protect against these risks while still preserving the benefits that featurization can provide.