THE CONVERGENCE OF HUMAN AND DIGITAL MEMORY: A CALL FOR CONSUMER ACTION

MICHAEL S. WAGNER†

As technology advances to provide consumers with more and more information, that technology comes close to effectively giving consumers the ability to converge their own memory with a digital memory. Technology today is capable of capturing almost every facet of a person's life—but only if the person lets it do so. Consumers must understand the depth that technology can pervade their lives and understand the real costs and risks associated with using that technology, including manipulation by the businesses developing the technology. Technology frequently outpaces governmental restrictions and law making—leaving it up to the consumers themselves to control the market and demand results sooner.

I. INTRODUCTION

What did you have for breakfast this morning? How did you sleep last night? Where did you go to lunch yesterday? Who did you eat with at lunch? Why did you eat lunch with that person? These questions are easy for many people to answer right now, but what about in a week, a month, or even a year from now? Not so easy. The discrete answers to these questions, however, often have little impact in individuals' lives. As the questions become more pervasive and comprehensive, the requisite answers begin to elicit more private information that some may be uncomfortable sharing, or even remembering for that matter. When people start to put together the answers to all of their questions, memories from that guide their behavior.

"We are our memories."[1] This often used quote elicits many thoughts and rests on possibly even more assumptions, but

† Michael Wagner is an attorney at Merchant & Gould in the firm's Denver, Colorado office practicing intellectual property and privacy law.

[1] *See* Lionel, *We Are Our Memories*, HUFFPOST HEALTHY LIVING (Nov. 17, 2011, 9:02 AM), http://www.huffingtonpost.com/lionel/we-are-our-memories_b_183489.html.

at its core one strong message persists: our memories are important to each of us and should be valued. Our memories cover a vast range of topics. In one way, memories form from our senses and perceptions. Five traditional senses that are well known are sight, hearing, taste, smell, and touch. There are also many other senses that we are able to perceive, such as balance, acceleration, and temperature. Beyond the senses, our memories are also composed of a vast array of complex structures that this author recognizes are far beyond his reach to fully explain. But at a practical level, there are many things that we remember, whether we want to or not. We have the ability to remember how to complete tasks or perform activities, such as riding a bike or driving to work every morning. We have memories of our emotions and feelings that we have had from past relationships, activities, and pursuits. Each of these memories helps shape our behaviors, guide our intuitions, and strongly influence our decisions on a daily basis.

While this simple introduction merely scratches the surface of the human memory, at a basic notion we are all aware of the power that our memories have on ourselves and our decisions. The idea of another person having control or access to our memories as a whole, or even the ability to manipulate our memories and emotions, should be alarming to most of us. In the past, such an idea has been nothing more than science fiction. Direct manipulation of another's thoughts is not currently a technology that has been developed.[2] As a result, businesses and people alike must resort to using other forms of technology to understand and predict the behaviors of others.

The concept of others trying to manipulate our behavior, however, is not new.[3] For example, businesses have been tracking consumer habits for decades and have in turn been trying to manipulate buying behavior.[4] Supermarkets place certain items at eye level and on end caps. Other stores entirely arrange their

[2] However, some suggest that these science fiction ideas are getting closer to reality. *Mind Goggling*, ECONOMIST (Oct. 29, 2011), *available at* http://www.economist.com/node/21534748.

[3] Tal Yarkoni, *In Defense of Facebook*, TAL YARKONI BLOG (June 28, 2014), http://www.talyarkoni.org/blog/2014/06/28/in-defense-of-facebook.

[4] Peter Ubel, *Brain Control and Consumer Behavior*, FORBES (Jan. 3, 2013, 2:00 PM), *available at* http://www.forbes.com/sites/peterubel/2013/01/03/brain-control-and-consumer-behavior.

layout to encourage additional spending. Businesses are not alone in manipulating behavior. Almost everyone we interact with is trying to manipulate our behavior in one way or another.[5] As Professor Yarkoni eloquently summarized:

> Your mother wants you to eat more broccoli; your friends want you to come get smashed with them at a bar; your boss wants you to stay at work longer and take fewer breaks. We are always trying to get other people to feel, think, and do certain things that they would not otherwise have felt, thought, or done.[6]

This type of research, development, and manipulation can only be based on observable behaviors and habits. But when our observable behaviors converge with the entirety of our memories, the pervasiveness of the manipulation by others crosses into a new realm that was previously unavailable. This article highlights the growth of particular consumer technologies that are bringing us closer to such a convergence and calls attention to the problems that may result.

II. THE CONVERGENCE OF MEMORY THROUGH TECHNOLOGY

Technology advances at such a rapid pace that by the time this article is being read, many of the following technologies may already feel outdated. Nevertheless, the consumer technologies currently being released and those likely to be released present the potential to collect an unprecedented amount of data from their users. As this amount of data continues to grow in both form and quantity, it forms a "digital memory" that begins to converge with discrete pieces of our own memories. With advancements in both computing and understanding of the human cognizance, technology moves ever closer to making the same connections and relationships to these discrete pieces of data as the human brain.

[5] Yarkoni, *supra* note 3.

[6] *Id.*

A. Modern Smartphone Apps

The most well-known data-collecting consumer product is the smartphone. The smartphone technology itself is capable of collecting and remembering many of the same senses that its users have. Take the iPhone 6 for example.[7] The iPhone 6 has a camera to capture both photos and videos—equivalent to the sense of sight.[8] The iPhone 6 similarly has a microphone to capture sounds—equivalent to the sense of hearing.[9] In addition, the iPhone 6 has an accelerometer that is capable of tracking and recording movement in the form of acceleration and balance.[10] The iPhone also has multiple ways to track the location of its users, including Global Positioning Systems ("GPS"), Wi-Fi assisted location, and cellular tower-based location.[11] And, of course, the iPhone has many ways for users to manually input data.[12] These features are now considered standard on most smartphones, but the new tracking programs and uses of data from these sensors create a new source of information that was previously unavailable.

In Apple's most recent major update to its operating system (iOS 8), Apple introduced a new "Health" feature.[13] Apple describes its new Health feature as follows:

> The new Health app gives you an easy-to-read dashboard of your health and fitness data. And we've created a new tool for developers called HealthKit, which allows all the incredible health and fitness apps to work together, and work harder, for you. It just might be the beginning of a health revolution.[14]

[7] *See iPhone 6*, APPLE, https://www.apple.com/iphone-6 (last visited Feb. 19, 2015).

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Health: An Entirely New Way To Use Your Health and Fitness Information*, APPLE, https://www.apple.com/ios/whats-new/health (last visited Feb. 19, 2015) [hereinafter *Health*].

[14] *Id.*

One goal of the Health feature is to provide a "really accurate answer" to the question "how are you?"[15] To attempt to answer that question, Apple boasts that:

> Heart rate, calories burned, blood sugar, cholesterol—your health and fitness apps are great at collecting all that data. The new Health app puts that data in one place, accessible with a tap, giving you a clear and current overview of your health. You can also create an emergency card with important health information—for example, your blood type or allergies—that's available right from your Lock screen.[16]

By having these types of data, Apple intends to let its consumers see their "whole health picture."[17]

This full view of one's health, on a constantly updated basis, has never been possible before, particularly in a consumer product carried by millions. What one may have previously considered sensitive health data may now be accessed by others, including businesses. There appears to be little question that Apple also encourages its users to share this data with others to make "[y]our health and fitness apps . . . work even harder for you."[18] Apple further advertises that:

> With HealthKit, developers can make their apps even more useful by allowing them to access your health data, too. And you choose what you want shared. For example, you can allow the data from your blood pressure app to be automatically shared with your doctor. Or allow your nutrition app to tell your fitness apps how many calories you consume each day. When your health and fitness apps work together, they become more powerful. And you might, too.[19]

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.*

While Apple also notes that the user has control of the data that is shared and that Apple encrypts its data,[20] it is unclear to both the users and to Apple itself exactly what happens to that data after it is shared.[21] As Apple cautions, "[a]pps that access HealthKit are required to have a privacy policy, so be sure to review these policies before providing apps with access to your health and fitness data."[22] To Apple's credit, it does require other apps that utilize HealthKit to have a privacy policy that follows particular guidelines.[23]

The privacy policies of other mobile applications, however, are often not clearly presented, or, in some cases, the apps are directly intended to mine the data of the user for other purposes.[24] For instance, a recent privacy enforcement survey of mobile apps conducted by the Global Privacy Enforcement Network ("GPEN") revealed that the privacy policies of many mobile apps are significantly flawed.[25] Several of the negative findings of the GPEN survey included:

- 85% of apps failed to clearly explain how personal information would be processed;
- 59% of apps did not clearly indicate basic privacy information (with 11% failing to include any privacy information whatsoever);
- 31% of apps were excessive in their permission requests to access personal information;

[20] *Id.*

[21] Though Apple requires apps accessing HealthKit to follow set privacy policy guidelines, it is up to the user to read the app's privacy policy and determine what the app does with the shared data. Apple is only able to require apps to disclose to users how the data will be used. *See id.*; *see also The HealthKit Framework*, APPLE, https://developer.apple.com/library/ios/documentation/HealthKit/Reference/HealthKit_Framework/index.html#//apple_ref/doc/uid/TP40014707 (last updated Feb. 2, 2015).

[22] *Health*, *supra* note 13.

[23] *The HealthKit Framework*, *supra* note 21.

[24] *See Privacy Sweep Has Shown a High Percentage of Apps Has Questionable Privacy Policies*, NORDVPN (Sept. 15, 2014), https://nordvpn.com/blog/privacy-sweep-has-shown-a-high-percentage-of-apps-has-questionable-privacy-policies [hereinafter *Privacy Sweep*].

[25] Rob Lister, McDermott, Will & Emery, *Global Privacy Enforcement Network (GPEN) Publishes Privacy Sweep Results*, NAT'L L. REV. (Sept. 29, 2014), http://www.natlawreview.com/article/global-privacy-enforcement-network-gpen-publishes-privacy-sweep-results.

- 43% of the apps had not sufficiently tailored their privacy communications for the mobile app platform—often instead relying on full version privacy policies found on websites.[26]

Many of the apps (75%) that were investigated also required at least one permission to access data on the user's device.[27] The most requested permission was access to the location of the user (32%), and other common permission requests were for device identification information (16%), and for access to other accounts (15%).[28] These types of privacy policies and practices illustrate that mobile apps are certainly not shy about collecting data from the user—often times for any possible use.

Even the simplest applications may sometimes be the culprits of such activities. Last year, the creators of what appeared to be merely a flashlight application, "Brightest Flashlight," were charged by the Federal Trade Commission ("FTC") for covertly harvesting and selling user location data.[29] The Brightest Flashlight app purported to be a "free" app, but in reality the Brightest Flashlight app secretly collected users' location information and device ID before users read and agreed to the app's privacy policy.[30] Moreover, the app misrepresented the user's preferences regarding data collection.[31] After collecting the data, the developers of the application turned around and sold the data to a data aggregator.[32] Prior to the FTC enforcement, the Brightest Flashlight app was ranked as one of the top free applications on the mobile store and had been downloaded tens of millions of times.[33]

[26] *Id.*

[27] *Privacy Sweep*, *supra* note 24.

[28] *Id.*

[29] *See, e.g.*, Complaint at 2, 4, *In re* Goldenshores Tech., LLC, No. 132-3087, 2013 WL 6512819 (F.T.C. Dec. 5, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/131205goldenshorescmpt.pdf; Shaun Nichols, *FTC Torches Android Flashlight App for Spying on Users*, REGISTER (Dec. 6, 2013, 1:42 PM), www.theregister.co.uk/2013/12/06/ftc_torches_android_flashlight_app_for_spying_on_users.

[30] *See* Nichols, *supra* note 29.

[31] *Id.*

[32] *Id.*

[33] Complaint, *supra* note 29, at 2.

B. Wearables

The emergence of wearable technologies opens up vast opportunities to collect data from users. One of the most controversial wearables is Google Glass, as shown below.[34]

Google Glass is currently equipped with many of the same features as a smartphone, and indeed is wirelessly connected to the user's smartphone.[35] Glass has a camera capable of taking both videos and pictures, a microphone for recording sound, an accelerometer to detect movements of the user's head, and location capabilities such as GPS.[36]

Despite having only similar features to a smartphone, Google Glass erodes some physical barriers and significant social barriers to collected data. The physical barriers themselves are quite minor. Prior to Glass, a user had to physically hold up a smartphone to capture pictures, video, or often audio. Now users can simply use hands-free controls to capture those items.[37]

The more significant impact of the introduction of Glass, however, is that there is no longer an act that is entirely discernable to a third-party that images, videos, or audio are being captured.[38] Holding up a smartphone and pointing it at an object or person to take a picture is a certain way to call oneself out in public, particularly if the user is taking a picture of another person. Even when the photograph is of an object, others still

[34] *Google Glass Goes to Back to the Drawing Board Under Nest [sic]*, GADGETREVIEW, (Jan. 15, 2015) http://www.gadgetreview.com/2015/01/google-glass-goes-to-back-to-the-drawing-board-under-nest.

[35] *See* Matt Swider, *Google Glass Review: Explorer Edition Upgrades to 2GB of RAM in the US and UK. Is It Worth the Price Now?*, TECHRADAR (Jan. 16, 2015), http://www.techradar.com/us/reviews/gadgets/google-glass-1152283/review.

[36] *Id.*

[37] *Id.*

[38] *See* Michael S. Wagner, *Google Glass: A Preemptive Look at Privacy Concerns*, 11 J. ON TELECOMM. & HIGH TECH. L. 475, 485–88 (2013).

generally notice that the act is happening. Glass removes these barriers. With Glass, it is possible to capture data without others noticing. Without such social barriers, the inherent conclusion is that data will be captured more frequently, with the potential to capture almost every perceivable bit of data that one comes across every day. One author, Mark Hurst, has referred to this type of capturing as "lifebits: the ability to record video of the people, places, and events around you, at all times."[39] Indeed, Google and third-party app developers promote almost non-stop data capturing to use the features of Glass to the fullest.

Google Glass is still developing as a consumer product, but third-parties have already developed over seventy apps for Glass.[40] Several of these apps already depend on extensive data collection to function. For instance, the "Where Did I Put" app seeks to function as your own memory for finding objects by asking Glass, "[r]emember where I put [the name of the object]."[41] Although it is still in a remedial stage, the concept itself is an early indicator of the power of Glass to converge with our own memories. Other interesting apps include Google Now, which provides "just the right information at the right time" by using location information and other data collected by Google, and Word Lens, which depends on analyzing what the user is seeing in real time to provide a translation of the words.[42] Although likely to be feature dependent, all this information could easily be stored and/or processed on the Cloud, such as Google or third-party servers, for later use by the user or anyone else with access to the data.[43]

Yet another growing type of wearable device is the so-called "activity tracker." These types of devices come in varying shapes and sizes and are intended to monitor and track movement by the user. One popular example of an activity tracker is the "Fitbit" brand activity tracker.[44] The newest model from Fitbit is the

[39] Mark Hurst, *The Google Glass Feature No One Is Talking About*, CREATIVE GOOD BLOG (Feb. 28, 2013), http://creativegood.com/blog/the-google-glass-feature-no-one-is-talking-about.

[40] *See, e.g.*, Iwan Uswak, *Google Glass Application List*, GOOGLE GLASS APPS, http://glass-apps.org/google-glass-application-list (last visited Apr. 30, 2015).

[41] *Where Did I Put App*, EXONOUS, http://exonous.com/wherediddiput.html (last visited Feb. 26, 2015).

[42] *Google Now*, GLASS, https://glass.google.com/u/0/glassware/10436347242727093239 (last visited Feb. 26, 2015); *Word Lens*, GLASS, https://glass.google.com/u/0/glassware/16789448588362059188 (last visited Feb. 26, 2015).

[43] *See* Wagner, *supra* note 38, at 487–89.

[44] *About Us*, FITBIT, http://www.fitbit.com/home (last visited Feb. 26, 2015).

"Surge," which is depicted below and described as a "Fitness Super Watch."[45]

This Fitness Super Watch tracks an exceptional amount of data from its users. For sensors and components, the Surge includes a GPS, three-axis accelerometers, a three-axis gyroscope, a digital compass, an optical heart rate monitor, an altimeter, an ambient light sensor, and a vibration motor.[46] With these components, the Surge tracks steps, distance, calories burned, stairs climbed, active minutes, sleep habits, continuous heart rate, location, distance, pace, elevation, and routes, among other calculable figures.[47] Remarkably, the Surge "[t]racks 7 days of detailed motion data–minute by minute" and tracks daily totals for the past thirty days.[48] The Surge also "stores heart rate data at 1 second intervals during exercise tracking and at 5 second intervals at all other times."[49] For tracking location, the sample rate for the GPS is one hertz.[50] Needless to say, the Surge tracks an impressive amount of data about the user. To keep track of all this information, the Surge also wirelessly and automatically synchronizes with smartphones and computers.

Fitbit and others are seemingly aware of the vast amount of data and use that as a prominent advertising point. In the Fitbit store, there is a software tool, Fitabase, that can be used to import

[45] *Surge*, FITBIT, https://www.fitbit.com/surge (last visited Feb. 26, 2015).

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *Id.*

data from the Fitbit device into research products.[51] The Fitabase software is described as "an innovative data platform that interfaces with web-connected consumer devices" that "can aggregate, analyze, visualize, and export data gathered from many device wearers."[52]

Another predicted type of activity tracker comes in the form of headphones.[53] Biometrics experts have suggested the ear is a desirable place to measure many data points about the human body, including a user's blood pressure, heart rate, electrocardiogram data, and core body temperature.[54] In addition, because headphones are already commonplace, users will be more likely to use such an activity tracker—greatly expanding the total amount of data collected by activity trackers.[55]

C. "Enchanted Objects"

Another substantial and rapidly expanding category of technology that has the potential to collect substantial amounts of data includes items associated with the Internet of Things, or as David Rose coined them, "enchanted objects."[56] Ordinary everyday objects are becoming "enchanted," or implanted with sensors and components that collect data about their users.[57] Rose describes some of these things as follows:

> Enchanted objects start as ordinary things—a pen, a wallet, a shoe, a light bulb, a table. The ordinary thing is then augmented and enhanced through the use of emerging technologies—sensors, actuators, wireless connection, and embedded processing—so that it become extraordinary. The enchanted object then gains some remarkable power or ability that makes it more useful, more

[51] Small Steps Labs, LLC, *Fitabase*, FITBIT, http://www.fitbit.com/apps/fitabase (last visited Feb. 22, 2015).

[52] *Id.*

[53] David Z. Morris, *Forget the iWatch. Headphones Are the Original Wearable Tech*, FORTUNE (June 24, 2014, 4:20 PM), http://fortune.com/2014/06/24/apple-beats-headphones-wearable-tech-biometrics.

[54] *Id.*

[55] *Id.*

[56] DAVID ROSE, ENCHANTED OBJECTS: DESIGN, HUMAN DESIRE, AND THE INTERNET OF THINGS xi–xiii (2014).

[57] *Id.* at 47–48.

> engaging, than its ordinary self. As the ordinary thing becomes extraordinary, it evokes an emotional response from you and enhances your life.[58]

Some have suggested that the Internet of Things will include twenty-six billion units installed by 2020, generating revenue exceeding $300 billion.[59] The rise of enchanted objects will unquestionably grow the amount of data collected on consumers, including data on even the most routine activities of a user's life.

The Livescribe pen, created by Anoto, is one example of an enchanted object.[60] Anoto took an ordinary pen and transformed it into something extraordinary. The most recent model of the Livescribe, the Livescribe 3 Smartpen, works as a regular ballpoint pen, but when paired with a smartphone or tablet, the user is able to "experience the magic it delivers."[61] The Livescribe smartpen integrates an infrared camera, ARM processor, Bluetooth Smart Chipset, flash memory and lithium ion battery to "bring your notes to life."[62] With these components, the smartpen is able to capture all the notes that are taken with it, store those notes, and transfer them to the user's smartphone or computer.[63]

D. Social Media

In a time long, long ago, people would have had to write down their thoughts and feelings in an archaic contraption commonly referred to as a diary or journal. Those thoughts were secured by the fact that they were only recorded in one place—a single book, written in ink on paper. Today, the thoughts that many people previously wrote in their journals are being tracked or seemingly freely shared with others. Not only could such a task be accomplished directly with a Livescribe pen, but social media

[58] *Id.* at 47.

[59] *HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack*, HP (July 29, 2014), http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.VK7q-SvF-Ck [hereinafter *HP Study*].

[60] ROSE, *supra* note 56, at 48.

[61] *Livescribe 3 Smartpen*, LIVESCRIBE, http://www.livescribe.com/en-us/smartpen/ls3 (last visited Feb. 26, 2015).

[62] *Features*, LIVESCRIBE, http://www.livescribe.com/en-us/smartpen/ls3/features.html (last visited Feb. 26, 2015).

[63] *Livescribe 3 Smartpen*, *supra* note 61.

has provided a commonplace platform for sharing one's thoughts and feelings.

Users of social media may even be unaware of the information that they are directly providing to social media platforms. Facebook, for example, provides users with the opportunity to supply almost an endless amount of information about themselves. Facebook even tracks what users do not actually choose to post.[64]

There is also no short list of social media platforms—Wikipedia lists over 200 currently available social networking sites.[65] Some of the more popular ones are briefly mentioned here. Snapchat allows users to capture any image they want and send those pictures to their friends (and the Snapchat servers).[66] Twitter allows users to share their quickest thoughts.[67] LinkedIn creates a platform to share all of your qualifications, business experience, and even your business network, along with what your network thinks about you and what you think about them.[68] Tumblr, Instagram, Flickr, and Vine all allow users to post or otherwise share photos and video.[69] Pinterest lets its users share almost any content from the web or from the user's own collection or creation.[70]

Each of these social media sites allows its users to record their memories, perceptions, and reactions. Over time, these digital memories and reactions are collected and analyzed, similar to one's own memories. While it assumed that most users will have some type of personal "filter" concerning what one is willing to share, there are no well-defined limits as to what these mental filters should include. As a result, consumers are left to guess what consequences will result from their own personally chosen filters.

[64] Casey Johnston, *Facebook Is Tracking What You Don't Do on Facebook*, ARSTECHNICA (Dec. 16, 2013, 1:40 PM), http://arstechnica.com/business/2013/12/facebook-collects-conducts-research-on-status-updates-you-never-post.

[65] *List of Social Networking Sites*, WIKIPEDIA, http://en.wikipedia.org/wiki/List_of_social_networking_websites (last modified Mar. 15, 2015, 5:48 PM).

[66] *Privacy Policy*, SNAPCHAT, https://www.snapchat.com/privacy (last updated Nov. 17, 2014).

[67] *About Twitter*, TWITTER, https://about.twitter.com (last visited Feb. 26, 2015).

[68] *User Agreement*, LINKEDIN, https://www.linkedin.com/legal/user-agreement (last visited Feb. 19, 2015).

[69] *Sign Up*, FLICKR, http://www.flickr.com (last visited Feb. 26, 2015); *Capture and Share the World's Moments*, INSTAGRAM, http://www.instagram.com (last visited Feb. 26, 2015); TUMBLR, http://www.tumblr.com (last visited Feb. 26, 2015); *Explore a World of Beautiful, Looping Videos*, VINE, http://www.vine.co (last visited Feb. 26, 2015).

[70] PINTEREST, http://www.pinterest.com (last visited Feb. 26, 2014).

The list of objects, devices, and platforms discussed in this section certainly does not fully cover the massive range of consumer products providing new ways to track consumers' data. But these products demonstrate the massive collection possibilities that products like these are having on consumer data collection. As discussed in the next section, people and businesses want to use this data, and consumers need to be prepared to respond.

III. A Necessary Consumer Response for Prevention

Due to the rapidly increasing amount of data that is being collected about consumers from the technologies described in the previous section, it is important for consumers to continue expressing their concerns to keep their data private and within their control. Through market forces, consumers have already made progress towards these goals, and in the face of growing data collection, those efforts need to continue. In general, consumers still consider their own memories and thoughts to be private, but with the convergence of collected and consumers' actual memories, the difference between the two grows more unclear.

A. People Want Your Data

Amassing vast amounts of information results in an expansion of our digital memories.[71] The more robust a consumer's digital memory, the easier it will be to manipulate the user. That statement is backed by the common knowledge of what most of us already know: the more you know about someone, the better your negotiating position. This idea is certainly not new; however, the tools that are being used to collect the data are new.[72] Even with the new tools, activities today continue to confirm the core concept: people want data from you and that data can be used against you.

Whether data use is for the more common market analysis by businesses or for the more sinister "entertainment" value for hackers, the recent past has shown that both uses continue to grow. In 2014, multiple photo hacks were identified that were

[71] Daniel Solove was one of the first to address a similar concept, which he refers to as a person's "digital dossier." DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 1–10 (Jack M. Balkin & Simone Noveck eds., 2004).

[72] *See* Zeynep Tufekci, *Facebook and Engineering the Public* , MEDIUM (June 29, 2014), https://medium.com/message/engineering-the-public-289c91390225.

apparently nothing more than a whim of the hackers. The most publicized of these hacks was that of several celebrities' Apple iCloud accounts.[73] The hacks resulted in the release of hundreds of intimate photographs of celebrities, including nude photos of Jennifer Lawrence, Kate Upton, Justin Verlander, Mary Elizabeth Winstead, Jessica Brown Findlay, Kaley Cuoco, and Kirsten Dunst.[74] Each of those celebrities confirmed the authenticity of the photos that were released.[75] The celebrity accounts were hacked and the photos were released on the image sharing site 4Chan.[76] Certainly, each of those celebrities thought that the photos that they had taken and stored in an on-line database were secure. After their release, however, the celebrities realized that they were not as secure as they once thought.[77]

In another photo leak that received less attention (likely due to less of a nude celebrity shock factor), over 98,000 photos from users of the Snapchat mobile application were released.[78] The incident was nicknamed "The Snappening."[79] Peculiarly,

[73] *Apple To Tighten iCloud Security After Celebrity Leaks*, BBC (Sept. 5, 2014), http://www.bbc.com/news/technology-29076899.

[74] *See* Amy Duncan, *Downton Abbey Star Jessica Brown Findlay Is Latest Naked Photos Victim as Her Sex Tapes Emerge Online*, METRO (Sept. 1, 2014, 11:03 PM), http://metro.co.uk/2014/09/01/downton-abbey-star-jessica-brown-findlay-is-latest-naked-photos-victim-as-her-sex-tapes-emerge-online-4853610; Josie Ensor, *Nude Jennifer Lawrence Photos Leaked by Hacker Who Claims To Have 'Private Pictures of 100 A-listers'*, TELEGRAPH (Sept. 1, 2014, 4:59 PM), http://www.telegraph.co.uk/news/celebritynews/11067182/Nude-Jennifer-Lawrence-photos-leaked-by-hacker-who-claims-to-have-private-pictures-of-100-A-listers.html; David McCormack et al., *Kirsten Dunst Leads Celeb Anger at Apple over Hacked Photos*, DAILY MAIL (Sept. 2, 2014, 7:35 AM), http://www.dailymail.co.uk/news/article-2740034/Kirsten-Dunst-leads-criticism-company-actively-investigates-claims-hundreds-stars-nude-images-stolen-iCloud.html; Jenn Selby, *Mary E. Winstead Naked 4Chan Photo Leak: 'To Those Looking at Photos I Took with My Husband, Hope You Feel Great About Yourselves'*, INDEPENDENT (Sept. 1, 2014), http://www.independent.co.uk/news/people/mary-e-winstead-nude-photo-leak-to-those-looking-at-photos-i-took-with-my-husband-hope-you-feel-great-about-yourselves-9704329.html; *Kate Upton Vows Legal Action After Leaked Nude Photos with Justin Verlander,* DET. FREE PRESS (Sept. 2, 2014, 11:58 AM), http://www.freep.com/article/20140901/SPORTS02/309010170/justin-verlander-kate-upton-photos.

[75] *See id.*

[76] Warwick Ashford, *Nude Celebrity Hack Forces Changes at Apple and 4Chan,* COMPUTER WEEKLY (Sept. 5, 2014, 9:44 AM), http://www.computerweekly.com/news/2240228236/Nude-celebrity-hack-forces-changes-at-Apple-and-4Chan.

[77] *See id.*

[78] Lorenzo Franceschi-Bicchierai, *98,000 Hacked Snapchat Photos and Videos Posted Online,* MASHABLE (Oct. 13, 2014), http://mashable.com/2014/10/13/the-snappening-photos-videos-posted.

[79] *Id.*

these photos were also released on the image-sharing site 4Chan.[80] In this case, users also presumably thought the photos that they took were secure, particularly due to the nature of the Snapchat service (allowing users to send a picture that "disappears" after a few seconds).[81] But Snapchat itself was not the one to blame for this incident.[82] Snapchat's servers were never hacked.[83] Rather, a third-party application that was intended to allow users to save images that were supposed to disappear had its servers hacked.[84] This hack in particular is a reminder that third-party apps often have access to primary applications on consumer devices, and those third-party apps often do not have the same security measures as the primary app that consumers largely associate with collecting their data. Even Snapchat itself warned its users not to use third-party services.[85]

Consumer device hacks were not limited simply to smartphones and applications either. Devices deemed part of the Internet of Things are also vulnerable to hacks, and a recent study suggests that seventy percent of such devices are vulnerable to hacking.[86] The Internet of Things devices averaged twenty-five vulnerabilities per product, and the products tested—along with their cloud and mobile application components—included televisions, webcams, home thermostats, remote power outlets, sprinkler controllers, hubs for controlling multiple devices, door locks, home alarms, scales, and garage door openers.[87] Making matters worse, ninety percent of the devices tested collected at least one piece of personal information.[88] Many of the devices had limited password requirements, if any, and did not encrypt transmissions, web interfaces, or software updates.[89]

[80] *Id.*

[81] Rheana Murray, *What Really Happens to Your Deleted Internet Messages and Photos*, ABCNEWS (May 9, 2014), http://abcnews.go.com/Technology/deleted-snapchat-photos/story?id=23657797.

[82] Franceschi-Bicchierai, *supra* note 78.

[83] *Id.*

[84] *Id.*

[85] *Third-Party Applications and the Snapchat API*, SNAPCHAT BLOG (Oct. 14, 2014, 8:23 AM), http://blog.snapchat.com/post/99998266095/third-party-applications-and-the-snapchat-api.

[86] Katie Nelson, *70 Percent of Internet of Things Devices Are Vulnerable to Hacking, Study Says*, MASHABLE (Aug. 2, 2014), http://mashable.com/2014/08/02/internet-of-things-hacking-study.

[87] *HP Study*, *supra* note 59.

[88] *Id.*

[89] *Id.*

Among the more humorous hacks of the Internet of Things, "smart toilets" were recently determined to be vulnerable to hacks.[90] By hacking the toilet, the hacker can control the functionality of the toilet with almost any smartphone with Bluetooth capabilities, including making the toilet flush, moving the seat up and down, and spraying the bidet.[91] Less entertaining hacks included hacking automated home systems[92] and baby monitors.[93]

Hacks are unmistakable examples of others wanting your data. Nevertheless, hacks serve as important reminders that anything that we put into a smart device is potentially available to others. Being able to trust the security techniques implemented into our smart devices should be a priority, especially with the quickly growing masses of information that we provide to our smart devices.

Hacks are not the only way that your data is being exposed to others. The same companies that provide us with our devices and services use the data we provide them to their advantage. Directed advertising based on consumer data has long been known and unfortunately almost become commonplace.[94] Yet, the pervasiveness of directed advertising is still growing—AT&T is currently looking for new and improved ways to more comprehensively track its users using an "unkillable" tracker.[95] Companies may also analyze consumer data for their own studies, blog posts, or other advertising purposes. For example, following the 2014 earthquake in Napa Valley, a popular fitness-tracker company, Jawbone, published the study "How the Napa

[90] Kashmir Hill, *Here's What It Looks Like When a 'Smart Toilet' Gets Hacked*, FORBES (Aug. 15, 2013, 3:55 PM), http://www.forbes.com/sites/kashmirhill/2013/08/15/heres-what-it-looks-like-when-a-smart-toilet-gets-hacked-video.

[91] *Id.*

[92] Kashmir Hill, *When 'Smart Homes' Get Hacked: I Haunted a Complete Stranger's Home Via the Internet*, FORBES (July 26, 2013, 9:15 AM), http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack.

[93] Kashmir Hill, *How a Creep Hacked a Baby Monitor To Say Lewd Things to a 2-Year-Old*, FORBES (Aug. 13, 2013, 6:35 PM), http://www.forbes.com/sites/kashmirhill/2013/08/13/how-a-creep-hacked-a-baby-monitor-to-say-lewd-things-to-a-2-year-old.

[94] Elizabeth Dwoskin, *FTC Recommends Limits on Data Collection Via Internet of Things*, WALL ST. J. DIGITS (Jan. 27, 2015, 1:20 PM), http://blogs.wsj.com/digits/2015/01/27/ftc-recommends-limits-on-data-collection-via-internet-of-things/?mod=WSJBlog&mod=blogmod.

[95] Kashmir Hill, *Find Out Whether This Unkillable Tracker Is on Your Smartphone*, FORBES (Oct. 28, 2014, 3:14 PM), http://www.forbes.com/sites/kashmirhill/2014/10/28/find-out-whether-this-privacy-killing-super-cookie-is-on-your-phone.

Earthquake Affected Bay Area Sleepers" on its blog.[96] The study revealed that ninety-three percent of users within fifteen miles of the epicenter were awoken when the quake struck.[97] What was potentially more revealing about this study was the fact that Jawbone saves and analyzes a substantial amount of the data collected by the fitness devices worn by its users. The study states that it "was based on thousands of UP wearers in the Bay Area who track their sleep using UP by Jawbone."[98] Jawbone even has its own "Data Science" team.[99] Two recent incidents in 2014, however, provided a new insight into more pervasive and manipulative studies that are being performed on consumers without their knowledge.

The first incident involved the social media giant Facebook. Facebook conducted a study to determine what effect emotional expressions in News Feeds have on its users. The study, titled "Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks," describes its significance as follows:

> We show, via a massive (N = 689,003) experiment on Facebook, that emotional states can be transferred to others via emotional contagion, leading people to experience the same emotions without their awareness. We provide experimental evidence that emotional contagion occurs without direct interaction between people (exposure to a friend expressing an emotion is sufficient), and in the complete absence of nonverbal cues.[100]

The experiment was described in the paper as follows:

> The experiment manipulated the extent to which people (N = 689,003) were exposed to emotional expressions in their News Feed. This tested whether

[96] Eugene Mandel, *How the Napa Earthquake Affected Bay Area Sleepers,* JAWBONE BLOG (Aug. 25, 2014), https://jawbone.com/blog/napa-earthquake-effect-on-sleep.

[97] *Id.*

[98] *Id.*

[99] *Id.*

[100] Adam D. I. Kramer et al., *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 Proc. Nat'l Acad. Sci. 8788, 8788 (2014), *available at* http://www.pnas.org/content/111/24/8788.full.

> exposure to emotions led people to change their own posting behaviors, in particular whether exposure to emotional content led people to post content that was consistent with the exposure—thereby testing whether exposure to verbal affective expressions leads to similar verbal expressions, a form of emotional contagion. People who viewed Facebook in English were qualified for selection into the experiment. Two parallel experiments were conducted for positive and negative emotion: One in which exposure to friends' positive emotional content in their News Feed was reduced, and one in which exposure to negative emotional content in their News Feed was reduced. In these conditions, when a person loaded their News Feed, posts that contained emotional content of the relevant emotional valence, each emotional post had between a 10% and 90% chance (based on their User ID) of being omitted from their News Feed for that specific viewing.[101]

In other words, researchers at Facebook, in conjunction with researchers at Cornell University, manipulated the emotions of its users by controlling what Facebook users saw in their News Feeds.

The second incident involved the dating website OkCupid.com ("OkCupid"). OkCupid now proudly states "We Experiment on Human Beings!"[102] The dating website performed various experiments from its "Love is Blind" experiment to its "The Power of Suggestion" experiment.[103] OkCupid's first experiment, "Love is Blind," looked to set up people without revealing their respective pictures to the other side—a type of virtual blind date.[104] They found that looks in an online profile

[101] *Id.* at 8788–89.

[102] Christian Rudder, *We Experiment on Human Beings!*, OKTRENDS (July 28, 2014), http://blog.okcupid.com/index.php/we-experiment-on-human-beings. Notably, the reason for OkCupid publishing these experiments was due to the Facebook incident discussed above. One of the founders of OkCupid stated that it seemed germane in light of the controversy surrounding the Facebook study. Nick Paumgarten, *Make Me a Match*, NEW YORKER (Aug. 25, 2014), http://www.newyorker.com/magazine/2014/08/25/2710913.

[103] Rudder, *supra* note 102.

[104] *Id.*

picture affected the conversation rate online, whereas if looks were only revealed in person, the looks had much less of an effect.[105] The study concluded "people are exactly as shallow as their technology allows them to be."[106] In OkCupid's second experiment, "So What's a Picture Worth," it looked to determine what a picture was worth on an online experiment.[107] It found that when users were allowed to rank others' profiles based on "personality" and "looks," most users ranked the profiles the same in both categories, even when the profile was nothing other than a picture.[108] OkCupid concluded from that experiment that a profile picture was worth vastly more than the text included in a user's dating profile.[109]

The third and final experiment published by OkCupid is the most controversial. In the third experiment, "The Power of Suggestion," OkCupid manipulated its "match percentage" to match up people who were actually predicted to be bad matches for one another. OkCupid determines a "match percentage" that indicates the likelihood that the two people would be a good match—the higher the percentage, the better the match. OkCupid wanted to test if its match percentages were actually working, or if it was simply the power of suggestion.[110] In other words, OkCupid wanted to verify that it was not the mere suggestion that people were a good match that resulted in successful relationships.[111] To test its suggestion, OkCupid took pairs of bad matches (thirty percent match) and told them they were exceptionally good for each other (displaying a ninety percent match).[112] OkCupid found that "[w]hen we tell people they are a good match, they act as if they are . . . [e]ven when they should be wrong for each other."[113] OkCupid also tested the reverse, telling people that they were bad for each other, when they were actually good.[114] The results: "the mere myth of compatibility works just as well as the truth."[115]

[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] *Id.*
[110] *Id.*
[111] *Id.*
[112] *Id.*
[113] *Id.*
[114] *Id.*
[115] *Id.*

Facebook's experiment and OkCupid's third experiment are particularly valuable examples of how businesses can collect data and directly use it to manipulate their users. There is little question that manipulation of consumers was the direct result of the experiments, although it was likely not the primary purpose of either experiment. Nevertheless, the manipulation occurred, and both companies were so proud of the results that they published them in a scientific journal and on their company blogs. What makes these examples especially interesting is that they were directly manipulating human emotions by exploiting the information users provided to the service. People assume that they are making their own decisions, but in reality many of their decisions are highly influenced by others, whether we recognize it or not. With emotions, we trust that what we feel is genuine and based on our previous experiences—our memories. As businesses are capable of manipulating consumers' digital memories, they in turn can manipulate consumers themselves.

B. Consumer Response to Data Exposure and Manipulation

Manipulation of consumers and exposure of their data is often not the first thought that a user has when the user decides to buy a product or service. The unfortunate reality of that unfamiliarity results in hidden information asymmetries that leave the consumer in a difficult position. Not only does the consumer not understand the full cost of the service or product, but also, at some level the consumer does not even fully understand the product or service that is being purchased.

Some have suggested that consumers, in fact, do understand that they are being researched and experimented on every time they use the Internet or any data-collecting product. Professor Yarkoni has stated, "I'm pretty sure most people do actually realize that their experience on Facebook (and on other websites, and on TV, and in restaurants, and in museums, and pretty much everywhere else) is constantly being manipulated."[116] Christian Rudder, founder of OkCupid, states that "[t]here's no question that Web sites experiment on people."[117]

While there might be some recognition that companies use consumer data for their own benefit, there is not a full

[116] Yarkoni, *supra* note 3.

[117] Paumgarten, *supra* note 102.

understanding about the level of manipulation that companies perform. Professor Yarkoni later admitted that his statement was "very clearly wrong."[118] Rather, Professor Yarkoni stated, "A surprisingly large number of people clearly were genuinely unaware that Facebook, Twitter, Google, and other major players in every major industry (not just tech—also banks, groceries, department stores, you name it) are constantly running large-scale, controlled experiments on their users and customers."[119]

We are entering, or perhaps have already entered, a new era of potential manipulation by businesses and exposure of consumer data. Basic directed advertising and product placement was an era that came years ago and is now seemingly here to stay. That era was sparked by "new" data tracking abilities such as the cookie or even consumer rewards cards. The new era of tracking we are entering now has similarly been triggered by "new" data tracking activities. New technology erodes previous barriers and allows a seemingly endless amount of data to be collected. We are now reaching a point where the depths of our own memories are beginning to converge with that of the digital memories that we allow to be recorded.

This convergence allows for an unprecedented spectrum of data exposure and consumer manipulation. Previous assumptions of technological limits and even ethical limits are no longer holding true. While most would have assumed the manipulation of his or her emotions by a free service was off-limits, that assumption is clearly no longer true as illustrated by both the Facebook experiment and the OkCupid experiment. The emotional manipulation exhibited in those studies was limited to data input into social media sites and dating sites. With the increase in data collected and monitored including physical health data, the possibilities grow at an exponential rate. For example, Facebook recently acquired Moves, an app that keeps track of exercise routines and places visited.[120] By augmenting its data collection, Facebook now has the ability to manipulate its users with even more data. As similar companies continue to grow, merge, and share data, an almost endless combination and correlation of data will become available.

[118] Yarkoni, *supra* note 3.

[119] *Id.*

[120] Lance Whitney, *Facebook Acquires Health and Fitness Tracking App Moves*, CNET (Apr. 24, 2014, 8:09 AM), http://www.cnet.com/news/facebook-acquires-health-fitness-tracking-app-moves.

If emotional manipulation is an acceptable business tool, the inquiry naturally focuses on what other types of manipulation are now (or soon will be) considered acceptable and enabled by new consumer technology. As discussed above, health tracking is becoming one of the most popular tools integrated into consumer products. Consumers have the ability to track almost all of their daily health statistics from the smartphone in their pocket or the watch on their arm. Businesses, such as Apple, Google, or FitBit, then have access to that data. Even more businesses may have access to this data if the user decides to share it, businesses decide to share or sell that data, or hackers gain access to that data. So, what happens when businesses decide to manipulate the health patterns of its users for its own edification? Will this be the next line that consumers all assumed would not be crossed until it actually is? With the advancement and widespread adoption of consumer technologies, such manipulation is surely possible. Companies, or anyone with access to this data, now have the ability to manipulate the user's digital memory to manipulate the user's actual experiences. As Dr. Tufekci has stated, these "new tools and *stealth* methods to quietly model our personality, our vulnerabilities, identify our networks, and effectively nudge and shape our ideas, desires and dreams" constitute "one of the biggest shifts in power between people and big institutions, perhaps the biggest one yet of 21st century."[121]

In a simplistic view, there are seemingly two options available to control or modify the potential manipulation and exposure of data: (1) have the public be fully informed about the manipulation and exposure of data, or (2) limit the type of manipulation possible. Neither of these options is likely achievable, nor is one inherently better than the other. But without government involvement, one practical process to work towards either option is controlled by consumers. Consumers have the ability to hold businesses accountable for their actions and behaviors by responding to data misuse by the companies to which they entrust their data.

The answer to how consumers hold businesses accountable, however, is rarely easy and often unclear. Professor Paul Ohm proposed an elegant solution to some privacy problems in his paper, "Branding Privacy."[122] Ohm's solution ties

[121] Tufekci, *supra* note 72.

[122] *See generally* Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907 (2013).

companies' privacy to their brands, and, in particular, to their trademarks.[123] Ohm's branded privacy focuses on a single company's abrupt change in its course of action regarding privacy, whether or not it clashes with the actions of competitors.[124]

As Ohm explains, trademarks are intrinsically tied to the goodwill of a company and encourage quality control through what some have called the "self-enforcing" nature of trademarks.[125] Trademarks, which are often the names of the company itself, are also difficult to change, and those changes often only come about when there is a significant or catastrophic event in a company's history or the company is looking to test a new business strategy.[126] Ohm proposes that privacy considerations should be intertwined with that of the trademark of company, such that if a company changes or abuses its privacy policy, it can lose its trademark.[127]

While Ohm's solution generally requires regulatory action to enforce his "branded privacy,"[128] some of the underlying theories in Ohm's solution do not require such extensive action. Indeed, government action may not be required at all.[129] Companies value their names and trademarks, and if consumers no longer associate those trademarks with the assurances guaranteed by the company and desired by the consumer, the company's brand will be injured. This does require that consumers actually raise the issue. Many have previously lamented over the fact that there is currently not a "market for privacy,"[130] but that does not mean it is impossible for consumers to affect the company's brand.

Indeed, there are already successful examples of that type of consumer effect on businesses. For example, partially in response the Facebook and OkCupid incidents discussed above, consumer response has already caused damage to those brands. Facebook received attention from many major publications

[123] *Id.* at 939.

[124] *Id.* at 953.

[125] *Id.* at 954.

[126] *See, e.g.*, Aaron Perzanowski, *Unbranding, Confusion, and Deception,* 24 HARV. J.L. & TECH. 1, 14–15 (2010).

[127] Ohm, *supra* note 122 at 962–63.

[128] *Id.* at 945–46.

[129] Even if this is not the case, consumer reaction likely will need to occur before government would even consider such regulations.

[130] Paul M. Schwarts, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices,* 2000 WIS. L. REV. 743, 763–71 (2000).

expressing the viewpoint that Facebook was wrong.[131] OkCupid similarly received negative criticism, including at least one author suggesting that the founder of the company is a sociopath.[132] OkCupid's comment section on its study similarly exploded with over 1200 responses—the majority of which were negative (although some are simply incomprehensible altogether).[133] In response to Facebook's experiment, Facebook has already changed its privacy policy to "something a human can actually read."[134] Its new policy is seventy percent shorter,[135] but it still explicitly states that it uses your information "for internal operations, including troubleshooting, data analysis, testing, research and service improvement."[136] In response to the celebrity photo hack, Apple increased its security measures.[137] Other companies have similarly been adversely affected when misusing consumers' data, including CarrierIQ,[138] NebuAd,[139] and Acxiom.[140]

In one of the first highly public battles over data misuse, Mircosoft's "Scroogled" campaign highlighted the potential for data misuse by Google.[141] Microsoft attempted to highlight the fact

[131] *See, e.g.*, Bruce Bower, *Main Result of Facebook Emotion Study: Less Trust in Facebook*, SCIENCENEWS (July 3, 2014), https://www.sciencenews.org/blog/scicurious/main-result-facebook-emotion-study-less-trust-facebook.

[132] Paumgarten, *supra* note 102.

[133] Rudder, *supra* note 102 (documenting angry customer commentary below the study blog post).

[134] Harrison Weber, *Facebook Turns its Data Policy into Something a Human Can Actually Read*, VENTUREBEAT (Nov. 13, 2014, 6:01 AM), http://venturebeat.com/2014/11/13/facebook-turns-its-data-policy-into-something-a-human-can-actually-read.

[135] *Id.*

[136] Kashmir Hill, *Facebook Added 'Research' to User Agreement 4 Months After Emotion Manipulation Study*, FORBES (June 30, 2014, 8:16 PM), http://www.forbes.com/sites/kashmirhill/2014/06/30/facebook-only-got-permission-to-do-research-on-users-after-emotion-manipulation-study.

[137] *Apple To Tighten iCloud Security After Celebrity Leaks*, *supra* note 73.

[138] Andy Greenberg, *Phone 'Rootkit' Maker Carrier IQ May Have Violated Wiretap Law in Millions of Cases*, FORBES (Nov. 30, 2011, 4:04 PM), http://www.forbes.com/sites/andygreenberg/2011/11/30/phone-rootkit-carrier-iq-may-have-violated-wiretap-law-in-millions-of-cases.

[139] Jacqui Cheng, *NebuAd, ISPs sued over DPI Snooping, Ad-Targeting Program*, ARSTECHNICA (Nov. 11, 2008), http://arstechnica.com/tech-policy/2008/11/nebuad-isps-sued-over-dpi-snooping-ad-targeting-program.

[140] Natasha Singer, *A Data Broker Offers a Peek Behind the Curtain*, N.Y. TIMES, Sept. 1, 2013, at BU1.

[141] *See, e.g.*, Mary Jo Foley, *Did Microsoft Just Kill its Anti-Google 'Scroogled' Campaign?*, ZDNet (Apr. 14, 2014, 4:06 PM), http://www.zdnet.com/article/did-microsoft-just-kill-its-anti-google-scroogled-campaign; *Scroogled*, WIKIPEDIA, http://en.wikipedia.org/wiki/Scro

that Google amasses large amounts of data from its users.[142] While many considered the campaign to be somewhat unsuccessful, it did create more public awareness and at least a glimmer of hope for a market for privacy and data misuse.[143]

As consumers continue to hold companies accountable for their actions regarding data misuse, the companies' respective brands will be injured. The types of data misuse include insufficient security measures, which result in hacks similar to the celebrity photo hack or the Snapchat-related photo hack. Other types of data misuse include manipulation of users based on their data, similar to that of OkCupid and Facebook. If there is to be any accountability for these types of data misuse, consumers need to continue responding to these issues and attempting to make sure that companies feel an appropriate effect from their actions. Now is "exactly the time to speak up!"[144]

IV. Conclusion

Manipulation of consumers' emotions, perceptions, and experiences and potential exposure to massive amounts of data should not become a regularly accepted principle of owning a smart consumer device or utilizing a social media platform. Yet, if consumers do not hold businesses accountable for their actions relating to data misuse, such types of manipulation and data exposure may become commonplace—similar to what is currently being seen with online directed advertising. Technology has advanced and continues to advance in a way that begins to blur the distinction between our own memories and perceptions and that of the digital memories that form from the collection of data by our consumer products. With coinciding advancements in cognitive understanding and correlative algorithms, those who have access to our digital memories face a minimal technological barrier to developing a pervasive understanding their consumers. From that understanding and the underlying data, businesses, and anyone with the same access, are able to manipulate consumers in unprecedented ways. If consumers hold the respective companies accountable for their misuse of data, the manipulation and exposure of data can be limited.

ogled (last modified Jan. 27, 2015, 6:40 AM).

[142] *Id.*

[143] *Id.*

[144] *Yarkoni, supra* note 3.