Privacy Lost: A Trip to the Mall

By Gary Renz and Albert J. Marcella, Jr.

The authors explore and reveal the incredible amount of information that is collected on individuals during a seemingly innocuous trip to the mall. The question: Is it privacy lost or information collected.

Question: how aware are you of the extent to which the most basic activities of your routine, daily life are tagged, tracked, analyzed, reviewed, sold, and stored in immense databases, creating a personal profile of you (a type of "digital DNA"), your friends, and your family (your social network)?

Every day, the government, private companies, and thieves try to collect, analyze, and aggregate—and sell—data about:

- Your restaurant and food preferences; your online and in-store purchases such as the styles and sizes of clothing you purchase and the cars, boats, and appliances you purchase
- Where you live and work, whether you rent or own and for how long; your occupation and who you work with
- Who you call and who calls you, how often and how long you talk, who you text and who texts you, what you say and type, who are your friends and Facebook "friends"
- Your physical characteristics, including your image, age, gender, eye and hair color, your facial wrinkles
- Your medical health, height and weight, the medications you purchase and are prescribed, medical diagnoses and medical concerns
- Your financial health, such as how your credit score changes over time, your credit and payment history, and financial solvency
- Where you drive, where you stop and park, where you walk, even where you will be 285 days from now
- Your work and home personal computers, tablets, smartphones, digital devices, and the information shared on those devices (called "cross-device tracking")[1]
- And much, much more

Your personal profile results from hundreds or thousands of companies and agencies routinely collecting large volumes of

1 Editorial (2013, October 9). Monitoring your every move. *The New York Times*. Retrieved from http://www.nytimes.com/2013/10/10/opinion/monitoring-your-every-move.html. Miller, C. C., & Sengupta, S. (2013, October 5). Selling secrets of phone use to advertisers. *The New York Times*. Retrieved from http://www.nytimes.com/2013/10/06/technology/selling-secrets-of-phone-users-to-advertisers.html. Sivaramakrishnan, K. (date unknown). The Drawbridge Cross Device Matching Technology. Retrieved from http://www.drawbrid.ge/technology.

tiny bits of data as we go about our personal (and now not so personal) lives. Data collection is occasionally done with approval and awareness, but increasingly collection is hidden and unauthorized. The resulting "big data" is statistically mined for patterns and useful linkages relating seemingly unrelated, isolated activities and characteristics—forming a digital mosaic of your life.

> Digital profiling…the process of collecting and compiling an individual's private and public digital DNA with the objectives of inferring (and with great probability potentially confirming) ownership and assigning characteristic attributes based upon an analysis of this digital DNA.

Still not yet convinced that you are losing your privacy? Think that this is just another Chicken Little, the "sky is falling," article? Then read on. By the article's end, we think you'll be convinced that you are being watched, tagged, tracked, recorded, and analyzed in ways you never suspected, never imagined but, certainly feared.

Driving to the mall

Ruth and her 13-year-old son Tom are going to a local shopping mall to shop for clothes and to buy food and decorations for Tom's upcoming birthday party. Upon leaving home, Ruth, sets the "away" mode to arm her home security surveillance system using the wireless key fob attached to her key ring. Driving her SUV equipped with GPS mapping and an automotive security and navigation service, Ruth winds her way through her neighborhood streets, passing a couple patrolling police cars, a school zone, and a mobile emissions testing vehicle. Ruth remembers that she should log into the website for the insurance company that sent her a monitoring device she plugged into her car's diagnostic port to get her driving score and find out if she can get a lower car insurance premium.

Ruth notices she is low on gas, so she stops at her favorite gas station. Ruth pays for the gas using her "affinity credit card" that gives money to her college alumni group. She also provides her gas loyalty rewards card number to get credits for the purchase. After passing several traffic lights, including rolling through a traffic light that had just turned red, Ruth enters the ramp onto the toll way that takes her to the mall in the neighboring town. Using the Speed Pass lane, Ruth easily bypasses the long lines waiting at the toll booths. In a hurry, Ruth fails to reduce her speed to 45 mph when passing through a construction zone, exiting the toll highway onto the mall access road, once again bypassing the toll booth using her Speed Pass.

Privacy lost or information collected

- The time Ruth left home, her security code, and other account information, such as house temperature and whether there are animals in the house. Time and temperature recorded by the home security system log which is transmitted to the security company's computers where it can be saved along with other information about Ruth's account.[2]
- The date, time, and route that Ruth took through her neighborhood. Obtained by community surveillance cameras, traffic light cameras, the car's GPS and navigation systems, and Ruth and Tom's mobile phones' GPS capabilities. Information can be stored in the car's computers, as well as Ruth and Tom's mobile phones, the mobile phone carrier's database, and the navigation assistance database.[3] Companies are promoting "intelligent street lights" that monitor many different types of activity, including smartphone addresses and high-definition audio and video. Such street lights could also monitor Ruth's route through video of her car and by tracking her smartphone.[4]
- Information about Ruth's toll highway travel including when and where entered and exited specific toll highways from which her average rate of speed can be calculated is obtained by the electronic toll collection system's cameras at ramp entrances or by sensors at the ramp entrance. This information is stored at the private contractor's office and/or the state highway department's information technology center after being transmitted wirelessly through cellphone towers.[5]
- The car's license plate number, which can be used to identify the car's make, model, year, vehicle identification number (VIN) number, and other vehicle information including owner, purchase price, current value, property taxes paid or due.[6] The status of the car's emissions is also known. Information is obtained by license plate scanning equipment on the police cars and by the roadside emissions testing vehicle, which also uses remote sens-

2 Examples of home automation, video surveillance, and fire and burglary protection features: http://www.vivint.com/en/ppc/security2?exid=20204&utm_source=google&utm_medium=cpc&utm_term={keyword}&utm_campaign=National%28Security%29+-+EC&mkwid={ifsearch:s}{ifcontent:c}OPTgVqve_d{device}&pcrid={creative}&pkw={keyword}&pmt={matchtype}&gclid=CKHfnpms-boCFSdp7AodXRcAaw#compChart & http://www.adt.com/media/home-security?ecid=rfresips000143&s_pid=1&s_kid=16407641&s_cid=157404428&s_agid=8673883148&s_aid=33497207948&s_ntwk=g&s_adp=1t1&s_ace=&s_plid=&s_dvc=c&gclid=CNao3oyr-boCFe5j7AodATwA9Q (retrieved on November 20, 2013) .

3 American Civil Liberties Union. Government location tracking: Cell phones, GPS devices, and license plate readers. Retrieved from https://www.aclu.org/government-location-tracking-cell-phones-gps-devices-and-license-plate-readers on November 24, 2013 and https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart retrieved on November 24, 2013. Hodgkinson, S. (2011). Is your city smart enough. *Ovum*. Retrieved from http://www.cisco.com/web/strategy/smart_connected_communities.html (see page 22 regarding community monitoring). http://mightygps.com/. https://www.onstar.com/web/portal/home?g=1. Malik, O. (2007, November 28). With Google's My Location, who needs a GPS? *Gigaom*. Retrieved from http://gigaom.com/2007/11/28/google-my-location/ on November 14, 2013. Sengupta, S. (2013, October 13). Privacy fears grow as cities increase surveillance. *The New York Times*. Retrieved from http://www.nytimes.com/2013/10/14/technology/privacy-fears-as-surveillance-grows-in-cities.html. Wikipedia. OnStar. Retrieved from http://en.wikipedia.org/wiki/OnStar on November 17, 2013.

4 Stanley, J. (2013, November 13). The three dimensions of the privacy apocalypse. American Civil Liberties Union. Retrieved from https://www.aclu.org/blog/technology-and-liberty-free-speech-national-security/three-dimensions-privacy-apocalypse on November 24, 2013.

5 Balasch, J. Rial, A., Troncoso, C. Geuens, C., Preneel, B. & Verbauwhede, I. (2010). PrETP: Privacy-Preserving Electronic Toll Pricing. http://cosic.esat.kuleuven.be/road_charging/contact.html. Wikipedia. Electronic toll collection. http://en.wikipedia.org/wiki/Electronic_toll_collection (retrieved on August 10, 2013). https://www.e-zpassny.com/en/home/index.shtml & https://www.ezpassva.com/ (retrieved November 20, 2013).

6 Weinsier, J. (2011, July 22). Florida makes $63 million selling drivers' info: Judge says info selling is legal. http://www.local10.com/news/Florida-Makes-63M-Selling-Drivers-Info/-/1717324/3078462/-/5juh04z/-/index.html. Retrieved on November 15, 2013.

ing equipment to measure vehicle emissions as they drive past.[7] The information could be stored at the state department of motor vehicles, the highway department, and the police department.

- The type and quantity of gas Ruth purchased and the amount of time since her last gas purchase, Ruth's credit card and gas loyalty card numbers that refer to account information (e.g., customer name, address, phone number, vehicle information, and gas and services preferences), outstanding credit card balance and remaining credit, credit card approval, zip code for billing address (if used as security protection to minimize fraudulent use of credit card). Information stored on the credit card and loyalty card issuers' computers.[8]
- Information about Ruth going through a red light and her speed while driving through the construction zone and the school zone. This information is obtained by automated red-light traffic enforcement and automatic speed enforcement monitoring equipment. The information is stored on computers at the private company hired to install and run the equipment. The company collects the information, which it forwards to the highway patrol and local police departments, as well as the district attorney's office. Ruth will eventually receive a ticket in the mail with instruction to access a website to view a video clip of her "stoplight roll" to validate the ticket she has received.[9]
- The status of the car's many computerized systems, including her acceleration rate, braking, and speed. Sent through the automobile's security and navigation system that monitors the automobile's systems for possible problems,[10] this information may be recorded and stored on the security and navigation system provider's computers.
- The number of miles Ruth drives each day, how often and how hard she brakes, how fast she accelerates, and how often she drives between midnight and 4 a.m., detailed information about how she drove on specific trips and an overview of Ruth's "driving habits." This information is obtained by the insurance company's telematic monitoring device that Ruth plugged into the car (called "telematics-based insurance" and is offered by several insurance companies).[11] The information is sent back to the insurance company and analyzed to determine how likely Ruth is to have an accident and to estimate the costs of the accident. This information is stored on company computers for an unknown amount of time. In addition, when she obtained the monitoring device, Ruth told the insurance company her birthdate, contact information, and details about all the vehicles in her household.[12]
- In addition, an "event data recorder" in Ruth's car also collects and records information from the car's computers and sensors about Ruth's driving actions and the car's systems, although the amount of time recorded is only a few seconds at a time.[13]

In the mall

Entering the mall's parking lot, Ruth drives under an overhead mall sign that unknown to Ruth has high-resolution security cameras that take pictures of every car entering and leaving the parking lot. The mall is in a crowded neighborhood with little free parking, so Ruth drives to the mall's parking garage, which charges for parking. Ruth takes a parking ticket upon entering, knowing that stores in the mall will validate the ticket if she and Tom purchase enough.

Ruth and Tom walk to the mall entrance, passing several security cameras without paying any attention to them. Upon entering the mall, they head immediately to the Mall Directory kiosk to locate Anderson's, a general merchandise department store with a reputation for carrying affordable young men's clothes. After locating the store on the store directory, Ruth points to its location on the mall map with her finger. Immediately, the digital display screen announces special events at Anderson's.

Privacy lost or information collected

- When Ruth's car arrived at the parking garage, her parking preferences (e.g., near main entrance and elevator, entered via South access road), and license number are re-

7 E.g., http://aircarecolorado.com/locations-and-maps/truck-locations/, http://www.imakenews.com/cppa/e_article002144019.cfm.

8 E.g., http://www.bp.com/en/global/corporate/press/press-releases/bp-launches-first-brand-wide-fuel-loyalty-program.html ; http://clintontwp.patch.com/groups/young-and-free-michigan/p/gas-station-loyalty-programs; http://www.slideshare.net/loyalmark/gas-rewards-program; http://www.tampabay.com/news/business/retail/rewards-program-offer-discounts-on-gas/2133241.

9 City of Chicago (2013, August 23). Automated speed enforcement cameras begin warning period. http://www.cityofchicago.org/city/en/depts/cdot/provdrs/traffic_signals_andstreetlights/news/2013/aug/automated_speed_enforcementcamerasbeginwarningperiod.html. FHWA Safety. Red-Light cameras/automated enforcement. Retrieved from http://safety.fhwa.dot.gov/intersection/redlight/cameras/ on November 18, 2013.

10 https://www.onstar.com/web/portal/home?g=1.

11 http://online.wsj.com/news/articles/SB10001424127887323420604578647950497541958; http://business.time.com/2013/08/06/big-data-is-my-copilot-auto-insurers-push-devices-that-track-driving-habits/; http://www.foxnews.com/leisure/2012/04/24/are-drivers-ready-for-big-brother-car-insurance-plans/; http://blog.creditkarma.com/personal-finance/car/review-progressive-snapshot-discount-rewards-you-for-driving-less-and-braking-softer/.

12 Brandon, J. (2012, April 24). Are drivers ready for Big Brother car insurance plans? Retreived from http://www.foxnews.com/leisure/2012/04/24/are-drivers-ready-for-big-brother-car-insurance-plans. Gallagher, J. (2013, January 20). Big Brother can lower your car insurance rate. Retrieved from http://www.stltoday.com/business/columns/jim-gallagher/big-brother-can-lower-your-car-insurance-rate/article_fcfb585e-6aaa-568c-bbc9-e1b33a399758.html. Progressive Insurance website: http://www.progressive.com/auto/snapshot-common-questions/ & http://www.progressive.com/auto/snapshot-how-it-works/. Scism, L. (2013, August 4). State Farm is there: As you drive. *The Wall Street Journal*. http://online.wsj.com/news/articles/SB10001424127887323420604578647950497541958. Sirota, D. (2012, August 15). Big Brother takes the wheel. Salon. http://www.salon.com/2012/08/16/big_brother_takes_the_wheel/ Tuttle, B. (2013, August 6). Big data is my copilot: Auto insurers push devices that track driving habits. *Time*. Retrieved from http://business.time.com/2013/08/06/big-data-is-my-copilot-auto-insurers-push-devices-that-track-driving-habits/. Troncoso, C., Danezis, G., Kosta, E., Balasch, J., Preneel, B. (2011). PriPAYD: Privacy-friendly pay-as-you-drive insurance. *IEEE Transactions on Dependable and Secure Computing, 8*, retrieved from http://cosic.esat.kuleuven.be/road_charging/contact.html.

13 Abraham, R. (2010, February 22). Is that a 'Black Box' in your car? *ABC News*. Retrieved from http://abcnews.go.com/Technology/MellodyHobson/car-black-box-records-key-data/story?id=9814181. Edelstein, S. (2012, August 14). NHTSA rules for "Black Box" event data recorders take effect September 1. *Digital Trends*. Retrieved from http://www.digitaltrends.com/cars/nhtsa-rules-for-black-box-event-recorders-to-be-released-september-1/ on November 18, 2013. MotorVehicleRegs.COM (2008, January 15). Event data recorders. Retrieved from http://www.motorvehicleregs.com/the_vehicle_reg_blog/2008/01/event-data-reco.html. Trop, J. (2013, July 21). A black box for car crashes. *The New York Times*. Retrieved from http://www.nytimes.com/2013/07/22/business/black-boxes-in-cars-a-question-of-privacy.html . Aald, M. L. (1999, May 30). Secret witness to car crashes in black boxes. *The New York Times*. Retrieved from http://www.nytimes.com/1999/05/30/us/secret-witness-to-car-crashes-in-black-boxes.html on July 20, 2013.

corded by high-resolution surveillance cameras.[14] Ruth's identity may also be ascertained from the car's license plate number. If the surveillance information is stored or analyzed and put into a customer analytics database, the garage owners can tell how often Ruth's car is parked in the parking garage.[15] This information may be stored in the garage's computer and can be combined in a database with other information, such as information collected by the mall.

- Ruth and Tom may be recorded by high-definition surveillance cameras in the mall and parking garage. For example, Ruth and Tom's gender, eye and hair color, height, estimated age and weight obtained by facial recognition of the images collected by security cameras and the camera in the Mall Directory kiosk.[16] They may also be personally identified using facial recognition software using publicly available pictures of either of them with their names, such as Ruth's or Tom's pictures on social media like Facebook, Instagram, Google, or Flickr.[17]
- Identification of and maybe access to Ruth and Tom's mobile smartphones through the mall's public Wi-Fi network, which their smartphones automatically linked to upon entering the mall because they had their phones Wi-Fi turned on. This access will also allow Ruth and Tom to be tracked through the mall as long as they are connected to the mall's Wi-Fi network.[18]
- Ruth's location in the mall is known because the parking ticket has a radio frequency identification (RFID) tag embedded on the back of the ticket.[19] The location of the parking ticket can be monitored until Ruth surrenders the ticket upon leaving the mall.

Entering the store, Ruth spies the new season's handbags and fashion accessories and stops to browse the items on display. Ruth is unaware of the high-resolution cameras recording and tracking her while she looks at different items as she walks through the store. In addition, if Ruth has uploaded the store's customer application, then the store can not only monitor Ruth's movements throughout the store, but the store can use Ruth's smartphone to direct her to in-store flash sales.

While standing in front of the handbags and accessories counter, Ruth unexpectedly receives a message on her phone with a coupon for a discount on specific bags and jewelry if she purchases them now. After initially walking away, Ruth quickly turns around and purchases a handbag she had not

14 http://www.3vr.com/products/videoanalytics/licenseplaterecognition.

15 See Kelly, H. (2013, April 26). After Boston: The pros and cons of surveillance cameras. *CNN Tech*. Retrieved from http://www.cnn.com/2013/04/26/tech/innovation/security-cameras-boston-bombings/; E.g., http://www.wrdw.com/home/headlines/Crews-install-high-tech-Greeneway-surveillance-cameras-228833421.html; http://www.security-expert.org/parkinglots.htm; http://www.videosurveillance.com/retail-surveillance-systems.asp; http://www.skywaysecurity.com/shopping-mall-security-camera-systems/.

16 McGinley, A. (2012, February 22). Bars, stores to use facial recognition technology to increase sales. Click Orlando. Retrieved from http://www.clickorlando.com/news/Bars-stores-to-use-facial-recognition-technology-to-increase-sales/-/1637132/8859986/-/1uomquz/-/index.html on November 18, 2013.

17 http://www.3vr.com/products/videoanalytics & http://www.3vr.com/products/videoanalytics/facialsurveillance. See http://www.slate.com/blogs/future_tense/2012/06/19/facebook_buys_face_com_will_mobile_facial_recognition_kill_privacy_.html and http://allthingsd.com/20110531/heres-what-really-scares-eric-schmidt-video/.

18 Clifford. S. & Hardy, Q. (2013, July 14). Attention, Shoppers: Store is tracking your cell. *The New York Times*. Retrieved from http://www.nytimes.com. http://euclidanalytics.com/product/index.html; retrieved November 1, 2013. http://www.retailnext.net/analytics-technology/data-acquisition; retrieved November 1, 2013 and http://www.retailnext.net; retrieved November 4, 2013. Francica, J. (2013, January 14). Attention Shoppers! Aisle411's indoor location app is a hit with top retailers. *Directions Magazine*. Retrieved from http://www.directionsmag.com/articles/attention-shoppers-aisle411s-indoor-location-app-is-a-hit-with-top-ret/303391. Grenoble, R. (2013, May 8). Euclid Analytics and retailers: How stores like Nordstrom track you via your smartphone's Wi-Fi signal. *Huff Post Business*. http://www.huffingtonpost.com/2013/05/08/euclid-analytics-nordstrom-retailers-tracking-smartphone_n_3237534.html. Hardy, Q. (2013, March 7). Technology turns to tracking people offline. *The New York Times*. http://bits.blogs.nytimes.com/2013/03/07/technology-turns-to-tracking-people-offline/ Hardy, Q. (2013, July 18). The rules of in-store surveillance. *The New York Times*. Retrieved from http://bits.blogs.nytimes.com/2013/07/18/the-rules-of-in-store-surveillance/?src=recg.

19 http://www.skidata.com/en/parking-management/tickets.html. See http://www.attraction-tickets.info/checking-out-the-new-rfid-disney-theme-park-tickets/; http://www.centralparking.com/managed/content/radio-frequency-identification-rfid. http://www.skyrfid.com/RFID_Parking_Management.php; http://www.timeparking.com/parking-control/radio-frequency-identification-rfid/#top.

intended to buy using the coupon she just received. At 25 percent off, it was impossible to resist.

Ruth pays for the handbag using her smartphone's "mobile wallet" application that uses Near Field Communication (NFC) to make purchases. Ruth pays by simply tapping her smartphone against the reader at the checkout register. The payment application also lets her apply the purchase to her hotel loyalty program.[20] After completing the purchase, a sales associate validates Ruth's parking garage ticket. Anderson's validates parking garage tickets as a courtesy to customers who spend over $100 during a single day. At every register, Anderson's has posted signs saying it tracks purchases during a visit by tracking names on credit card purchases. Alternatively, Ruth could have validated her parking ticket by showing her receipts to the garage attendant, who would optically scan to confirm the purchases.

20 https://www.google.com/wallet/shop-in-stores/index.html lists loyalty programs.

Privacy lost or information collected

- Ruth's taste in fashion, items examined, amount of time spent examining each item, interest level in items examined, and her response to the prices. Information is obtained by cameras that track Ruth's expression and her eye movement. By measuring the shopper's response to different designs, retailer can determine what caught Ruth's attention. This information is collected and stored in the retailer's database, which could be sold to manufacturers or other retailers.[21] Facial recognition systems exist that charge a person's account for purchases simply by recog-

21 http://www.retailnext.net retrieved on November 1, 2013. http://euclidanalytics.com/product/index.html retrieved on October 10, 2013. Lowe, M. C. (2013, August 1). Tracking your trade show. *Meetings and Conventions*, *48*. http://www.meetings-conventions.com/article.aspx?id=55276. http://www.sherpa-solutions.com/activmetrics/ retrieved on November 18, 2013. http://www.shoppertrak.com/ retrieved on November 18, 2013. http://aisle411.com/retailers/ retrieved on November 1, 2013.

nizing the person's face and which item was removed from a display.[22]

- Insight into Ruth's impulsivity to purchase items and her response or sensitivity to discounts. Information collected over time about how Ruth responds to coupons delivered "real-time" can be used to create a profile of her impulse purchases. For example, the tracking software tells the store that Ruth was looking for boy's clothing, but that she stopped for five minutes in front of the handbag and fashion accessories, bought a handbag after receiving a coupon offer after walking away and then returning within a couple minutes. [23]
- When Ruth uses her smartphone to pay for products, her bank or credit card account information, including account numbers and passwords or other authentication, will be obtained by the "near field communication" (NFC) device and recorded by the store, the application, and the payment processor.[24]

Ruth is unsure where the boy's clothing department is, so she uses a smartphone application that helps her locate departments and merchandise within a store. This in-store navigation device tells her the boy's clothing department is on the second floor at Anderson's and displays a route to get to the department. En route to the clothing department, Ruth and Tom stop to look at various displays, but they do not buy anything.

After reaching the clothing department, Ruth and Tom look around at the racks, shelves, and displays of clothes and accessories. Tom tries on some clothes. While Tom was trying on the clothes, Ruth looks at several boys' clothing displays. Ruth sees a couple of things she likes, but after looking at the price tags, she decides they are too expensive. While trying on clothes, Tom publicly Tweets that he is shopping at Anderson's and sends pictures of himself trying on the designer's clothing. He also posts his pictures ("selfies") to Instagram, a photo-sharing platform, and Google Plus. In his postings, Tom included #Anderson's and #designer's name which allow others to search on those terms and locate Tom's postings.

Ultimately, Ruth and Tom decide to buy two shirts, a pair of pants, a belt, and a jacket, all from the same clothing designer's line. Ruth pays for the clothes using her airline rewards credit card again. As they leave the clothing department, Ruth's phone beeps, indicating she has incoming messages. Opening the messages, Ruth gets directions to the designer's line of boys' shoes in the Anderson's shoe department using her in-store navigation application and a coupon for a 15 percent discount on the clothes she was looking at on the displays.[25] Ruth ignores the messages, but wonders how Anderson's knows so much about what she is looking at and purchasing. Ruth and Tom are unaware that they are being tracked in the store.

Privacy lost or information collected

- The route Ruth and Tom took through Anderson's, what stops they made and how long they spent in an area, even which items Ruth or Tom picked up to examine more closely and whether they looked at the prices. In addition, Anderson's knows the amount of time that Ruth and Tom spent in the clothing department, the items they examined, the items they purchased, and the items they didn't try on or purchase. This information is obtained by high-resolution surveillance cameras in Anderson's and tracking software that locates Ruth and Tom's smartphones in the store through the phones' Wi-Fi and GPS signals.[26]
- The in-store navigation and monitoring application will probably collect and record search requests and the shopper's movement through the store. This information is likely to be shared with the retailer and the application information may be sold to other companies.[27] Unlike covert tracking systems, this in-store navigation application was voluntarily installed by Ruth, so she consented to its tracking, even though she may not know the extent to which she is monitored.
- The clothing that Tom tried on had radio frequency identification threads stitched into the clothing, which responded to a transmitter when he entered the fitting room and at the register. The transmitter reported that certain items of clothing had been taken into the changing room. The sales people could use this information from the RFID tags to gather additional clothing and accessories to show Tom that would complement the items Tom took into the changing room.[28] Combined with information about what Tom and Ruth purchased, the store knows that certain clothing items ultimately did not appeal to Tom or Ruth, even though initially they were attracted enough to them to try them on.
- Personal information about Tom's preferences in clothing brand, size, color, and styles. Purchase information was obtained by the store's registers, which recorded what Tom purchased and that the purchases were on Ruth's credit card. Publicly posting the messages and pictures with hash tags alerted the store and designer that they were a topic

22 http://www.prweb.com/releases/2013/4/prweb10651215.htm.

23 http://iinside.com/.

24 See http://www.rfidjournal.com/articles/view?9105/ & http://lifehacker.com/5943006/what-is-nfc-and-how-can-i-use-it. https://www.google.com/wallet/shop-in-stores/index.html is a smartphone payment application.

25 Kurtovic, A. (2013, January 10). aisle411 showcases technology to identify customers as they enter a store. *St. Louis Business Journal*. Retrieved from http://www.bizjournals.com/stlouis/blog/BizNext/2013/01/aisle411-showcases-technology-to.html?ana=twt&utm_source=buffer&buffer_share=d2501 on October 15, 2013. See http://aisle411.com/solutions/publisher-solutions/ and http://aisle411.com/retailers/.

26 http://www.3vr.com/products/videoanalytics & http://www.3vr.com/products/videoanalytics/dwelltime .

27 Strom, D. (2013, June 6). GPS in retail stores helps convert browsers to buyers. *Solution Providers for Retail*. Retrieved from http://www.solutionprovidersforretail.com/ on November 18, 2013. See http://aisle411.com/drive-store-visits-loyalty-basket-size/ and http://www.esri.com/software/arcgis/extensions/trackinganalyst.

28 Video on RetailNext website (http://www.retailnext.net/, retrieved November 14, 2013).

in pictures or messages. By using facial recognition of the pictures, the store and designers, as well as anybody else tracking Tom's posts, can link images and texts to Tom, and maybe indirectly to his mother Ruth if she is mentioned in Tom's postings.[29]

- Anderson's may use the data it has collected to infer that Ruth has a son because Tom's clothing was purchased on Ruth's credit card, which may be combined with video surveillance showing Tom walking with Ruth through the store. If the software is connected to other databases, themay be able to match Ruth's credit card purchases with other records showing that Ruth has a son around Tom's age.

Ruth and Tom leave Anderson's to get something to eat in the mall. Using the Internet feature on her smartphone, Ruth searches the online mall directory to find out what restaurants are available in the mall. After choosing a fast-food restaurant from the list, Ruth clicks on the name to find its location. Her phone produces a map of the mall with direction on how to get to the restaurant from where she is presently located. Once there, Tom orders a meal, which Ruth pays for with cash.

While eating, Tom uses his smartphone to scan the QR (Quick Response) code on the meal receipt to see if he has won a free meal in a contest offered by the restaurant chain (a QR code is basically a graphic, similar to a barcode, that links to a website). Linked to the restaurant's website, his phone shows that he did not win a free meal. However, the link tells Tom that if he enters information about himself, he will get coupons for discounts on future meals at the restaurant chain, and can click an icon on his phone to locate the closest restaurant. Tom's phone then rings. After answering, Tom is asked if he is willing to complete a customer satisfaction survey about the restaurant meal he had just purchased.

Privacy lost or information collected

- Ruth's restaurant preference, including the restaurants on the list that Ruth did not select for directions, and the suggested route to the restaurant chosen. Ruth and Tom's actual route to the restaurant can be tracked through mall surveillance cameras and tracking software, through Ruth's phone if it is connected to the mall's Wi-Fi system, or the in-store navigation application may still be tracking Ruth as long as she is within the geographic "fence"

29 http://www.businessinsider.com/facebook-is-about-to-launch-a-huge-play-in-big-data-analytics-2013-5. Oremus, W. (2012, June 21). Facebook has automatically signed you up for facial recognition. Here's how to opt out. *Slate*. Retrieved from http://www.slate.com/blogs/future_tense/2012/06/21/facebook_facial_recognition_how_to_opt_out.html on November 23, 2013.

area.[30] These types of tracking software would also collect information on when and where Ruth stopped en route to the restaurant.

- The type and amount of food purchased at the restaurant, including specific items, quantities, and if the restaurant chain maintains records using debit card information, how often Ruth visits the restaurant and what items she purchases. The debit card information may be collected and stored by the bank and possibly the merchant.
- Tom's phone number and email address may have been sent to the restaurant chain when he scanned the QR code if the code planted software on his phone or the website sent cookies or other tracking software when Tom's phone linked to the site. This information will be maintained by the restaurant chain, but it may be sold to companies that aggregate such information, depending on the restaurant chain's privacy policy.[31]

Lunch finished, it's off to buy birthday party supplies at the One More Year party supplies store. On the way, Ruth stops to look at the mannequin in the window display of Rachel's Fashions, an upscale women's clothing store. Impatient, Tom says he is going ahead to a video game store to look at games. Ruth agrees and Tom heads off. Unknown to Tom, his mother turns on monitoring software she had installed on Tom's phone to track his activities.

Ruth goes into Rachel's Fashions to get a sense of the latest fashions, although she doesn't intend to buy anything. After looking for 10 minutes, Ruth leaves and walks toward One More Year to look at birthday supplies. Ruth is in no hurry since Tom is occupied, so she stops occasionally to look at several stores' window displays.

As she enters the One More Year store, Ruth calls Tom's smartphone to tell him she is at the birthday supplies store. Before calling Tom, Ruth checks the monitoring application to see where Tom has been and what calls and text messages he has sent and received. Although she decides not to, Ruth could also activate Tom's phone's camera and microphone to see and listen to his activities.

Privacy lost or information collected

- Ruth's taste in fashion, the clothing that she looked at in the window display and in the store, the amount of time she spent looking at each display item, and her reaction to the price, as well as her possible interest level in specific items. This information was obtained because Rachel's Fashions uses mannequins that have a high-resolution camera embedded into one eye. The camera feeds images into facial-recognition software that records and analyzes the images to determine the gender, race, and approximate age of people it sees, not only in the store but those looking at the store's window. The mannequin is placed in the store's window display to collect information that helps Rachel's Fashions decide which fashion items will likely draw people into the store. The information obtained from the mannequins can determine how long each person looks at each display (called "dwell").[32] In theory, a person's reaction to the display and price could be recorded using multiple software programs. For example, there is software that could use the images to assess people's response to store displays by recording facial expressions and eye movements.[33]
- Tom's text messages, emails, location in the mall, and potentially what he saw or heard when in the mall are known to Ruth. Ruth collected this information when she turned on the monitoring application for his mobile smartphone.[34] In addition, Tom's location and smartphone activities may be known to anybody monitoring his navigation application or other application on Tom's mobile phone that transmits information about his smartphone usage.[35] As long as Ruth or Tom's smartphone is turned on, it registers its location with cell towers every few minutes, data that is stored by mobile phone carriers for varying lengths of time.[36]

In the One More Year party supplies store, Ruth picks up several items that she needs for Tom's birthday party. Ruth signs up for the store's birthday club to get a 15 percent discount on all party items she is purchasing today. The club requires Ruth to give Tom's name, birthdate, gender, Ruth and Tom's email addresses, their home phone number and address, and Ruth's mobile phone number.

In addition to the immediate discount, the One More Year birthday program offers a 10 percent discount on future store purchases and provides Ruth and Tom with a list of children enrolled in the store's birthday program who live within five miles of Tom and are within a year of Tom's age. Using this

30 http://aisle411.com/retailers/.

31 Geer, D. (2013. August 19). The dangers of QR codes for security. *Data Protection*. Retrieved from http://www.csoonline.com/article/738366/the-dangers-of-qr-codes-for-security on November 18, 2013. Kieseberg, P., Leithner, M., Mulazzani, M., Munroe, L., Schrittwieser, S., Sinha, M., & Weippl, E. (2010). QR code security. *Fourth International Workshop on Trustworthy Ubiquitous Computing (TwUC 2010). Retrieved from* http://www.sba-research.org/team/researchers/peter-kieseberg/ *on November 12, 2013.* Lyne, M. (2009, October 15). What is a QR code and why do you need one? Search Engine Land. Retrieved at http://searchengineland.com/what-is-a-qr-code-and-why-do-you-need-one-27588 on November 1, 2013.

32 Ebhardt, T., Remondini, C., & Timberlak, C. (2012, November 22). Mannequins collect data on shoppers via facial-recognition software. *The Washington Post* with *Bloomberg*. Retrieved from http://articles.washingtonpost.com/2012-11-22/business/35510345_1_mannequins-facial-recognition-software-eyesee. Hill, K. (2012, November 28). Why do mannequins that spy on us creep us out? *Forbes*. Retrieved from http://www.forbes.com/sites/kashmirhill/2012/11/28/why-do-mannequins-that-spy-on-us-creep-us-out/. Stern, J. (2012, November 26). Department store mannequins are watching you. No, really. *ABC News*. Retrieved from http://abcnews.go.com/Technology/department-store-mannequins-watch-eyesee-analyzes-shoppers-webcams/story?id=17813441. See http://www.almax-italy.com/en-US/ProgettiSpeciali/EyeSeeMannequin.aspx.

33 See Cara by IMRSV at https://www.imrsv.com/learn.

34 http://www.mobile-spy.com/ retrieved on October 10, 2013. http://www.stealthgenie.com/index.html retrieved on November 22, 2013.

35 Miller, C. C., & Sengupta, S. (2013, October 5). Selling secrets of phone use to advertisers. *The New York Times*. Retrieved from http://www.nytimes.com/2013/10/06/technology/selling-secrets-of-phone-users-to-advertisers.html. Prindle, D. (2013, August 8). Find your phone with these helpful tracking tips. *Digital Trends*. Retrieved from http://www.digitaltrends.com/mobile/how-to-track-a-cell-phone/ on November 23, 2013. See Flurry's API and analytics at http://www.flurry.com/flurry-user-acquisition-analytics.html.

36 American Civil Liberties Union. Government location tracking: Cell phones, GPS devices, and license plate readers. Retrieved from https://www.aclu.org/government-location-tracking-cell-phones-gps-devices-and-license-plate-readers on November 24, 2013 and https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart retrieved on November 24, 2013.

list, Ruth and Tom then can choose which children they want to invite to Tom's party. One More Year will email each child chosen a customized party invitation to Tom's party and it will track the RSVPs from the children. Ruth can check the RSVP's through the personal email account she created on One More Year's website.

When Ruth pays for the items using her bank debit card, the store register generates a coupon for a 10-percent discount on any birthday cake purchased at the Fresh-as-Ever Bakery within two days, which is also located in the mall. The coupon has Ruth and Tom's names on it, as well as an identification code. Ruth decides to purchase a cake before leaving the mall using the coupon. To use the coupon, Ruth must show her driver's license to the clerk to confirm it is her coupon. The clerk looks at the picture and name on the license, confirming it is Ruth, and scans it quickly.

Privacy lost or information collected

- Personal information about Tom's birthdate, gender, age, home address and phone number, email address (in compliance with the Children's Online Privacy Protection Act), and that Ruth is his mother. Personal information is also obtained about Ruth, including her home address, phone number, email address, mobile phone number, and that she is Tom's mother. One More Year stores this information on its computer system and may sell this to data brokers.
- Tom's friends who are members of the One More Year birthday program. This information can be used to track Tom's social network of friends.
- Ruth's bank preference, checking account number, store location, the items purchased, and the amount paid are known to One More Year. Ruth's bank knows that she used the bank debit card to buy merchandise at One More Year.
- Fresh-as-Ever Bakery will learn Ruth and Tom's names when she redeems the coupon and shows her identification to use the coupon. In addition, her home address, height, and weight, picture, and driver's license number will be recorded by scanning the driver's license. One More Year and Fresh-as-Ever Bakery may exchange information on their customers, so One More Year will know the information from Ruth's driver's license scanned by Fresh-as-Ever Bakery and the bakery will know information collected by One More Year in the application form. The two sets of data can be linked by the identification code generated by One More Year.[37]

The day's purchases in hand, Ruth and Tom leave the mall and head to their car. Exiting the parking garage, Ruth hands the parking attendant her garage parking ticket, which had been validated by Anderson's. Ruth merges onto the tollway, paying once again with her Speed Pass, and heads toward home.

A mile from home, while stopped at a traffic light, Ruth uses her mobile phone application to turn on the exterior house lights and adjust the inside temperature, preparing the house for their arrival. Pulling into their garage, Ruth and Tom are finally home. As she enters the house, carrying bags of clothing and party supplies, Ruth types in her security alarm deactivation code.

37 For sharing information, see Valentino-Devries, J., & Singer-Vine, J. (2012, December 7). They know what you're shopping for. *The Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10001424127887324784404578143144132736214.

Privacy lost or information collected

- The time that Ruth and Tom left the mall's parking garage, how much time Ruth spent in the mall, and the fact that Ruth spent at least $100 at Anderson's because it validated her ticket. This information is recorded, stored, and probably analyzed by the parking garage, and maybe sold to third parties.
- The time and day that Ruth and Tom arrived home (and left the house when they enabled the security system) is recorded and stored by the home security system log of the time the alarm was disabled. The home security service has information about Ruth and her family obtained from her application and account information. This is stored on the security company's computers. The security company also has information about the temperature inside the house at all times and knows Ruth's temperature preferences at different times of the day. Garage openers using the Internet or smartphones would also record information about opening and closing the garage doors, and even turning on lights in the house.[38] Similarly, a "smart" home thermostat that can be controlled remotely by Internet or smartphone would also record information.[39] Energy history is also recorded on some smart thermostats.[40]
- The route Ruth took home was again recorded by the electronic toll collection system and surveillance cameras. As discussed earlier, the car route may also have been transmitted by the car's security and navigation system. The route home could be known by the mobile phone company because Ruth's smartphone transmitted (and maybe recorded) its location as it "pinged" cell towers or by its GPS capability.

Over the next few hours, Ruth's begins receiving text messages and emails.[41] From Anderson's she receives an announcement of their next sale and a discount coupon for the purse she admired. Fresh-as-Ever Bakery emails an offer to "like" them on Facebook and receive a two-for-one coupon good for coffee and a low-calorie muffin on her next visit. Salads n' Wraps, one of the restaurants in the mall that Ruth has never visited, sends her a coupon for a free meal with the purchase of another meal. The message suggests that Ruth may wish to try a healthier alternative the next time she is at the mall's food court.

Ruth receives an email from an online women's clothing website that Ruth had never heard of before. The email advertises low prices on the clothing designers' lines that Ruth was looking at in the mall. This seems rather strange to Ruth, but the prices are better than those she had just seen in the mall, so she does not delete the email. Later, in regular mail, Ruth receives a coupon for clothing similar to what she was looking at in the mall. [42]

Data aggregation compounds the privacy lost or information collected

One may think the privacy risks are relatively minimal if the information is only recorded, analyzed, and stored on each store's computer systems. Plus, Ruth volunteered much of the information, so she was aware that she was giving retailers useful information. In exchange, she got discounts and other services. Where's the harm? Well, as Natasha Singer wrote, "there is a fine line between customization and stalking."[43]

The data are valuable for creating detailed profiles of Ruth and Tom, especially when combined with other data, such as information from other stores, consumer credit databases, and public records. For example, Rachel's Fashions may not only keep information about Ruth on its computers, but it may also sell or give the information to clothing distributors, designers, or companies that specialize in aggregating customer data that is then sold to other companies ("data brokers").[44] Marketers particularly value detailed data that can be "data mined" for underlying patterns.[45] Government agencies, insurance companies, and lawyers may also find the data valuable for their own unique purposes.

Presently, there are few laws that restrict the collection, exchange, retention, or use of personal information relating to marketing data, although laws relating to consumer credit reports may apply.[46] Companies may voluntarily offer to limit dissemination in their privacy policies. But, those policies may also constitute waivers of a person's right to privacy regarding the information obtained with or without the person's consent. Policies most likely also state they may be changed at the company's discretion. Some data brokers and data analytic companies may also allow consumers to "opt-out" of data collection, analysis, and sharing such as Acxiom and Euclid Analytics.[47]

38 http://www.liftmaster.com/lmcv2/products/introducingliftmasterinternetgateway.htm.

39 http://yourhome.honeywell.com/home/Products/Thermostats/7-Day-Programmable/Wi-Fi+Smart+Thermostat.htm.

40 https://nest.com/blog/2012/10/02/the-next-generation-nest-thermostat/.

41 Singer, N. (2012, June 16). Mapping, and Sharing, the Consumer Genome. *The New York Times*. Retrieved at http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=0).

42 Olson, P. (2013, October 30). Meet the company that tracks more phones than Google or Facebook. *Forbes Magazine*. Retrieved from http://www.forbes.com/sites/parmyolson/2013/10/30/meet-the-company-that-tracks-more-phones-than-google-or-facebook). www.flurry.com; retrieved November 12, 2013.

43 Singer, N. (2012, June 16). Mapping, and sharing, the consumer genome. *The New York Times*. Retrieved from http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?pagewanted=2&_r=0.

44 See Valentino-Devries, J., & Singer-Vine, J. (2012, December 7). They know what you're shopping for. *The Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10001424127887324784404578143144132736214. http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=0. http://www.epsilon.com/about-us/our-story; http://www.datalogix.com/audiences/online, retrieved November 13, 2013; http://acxiom.com/resources/the-future-is-cross-channel-11-marketing-at-scale/; retrieved November 14, 2013.

45 Beckett, L. Everything we know about what data brokers know about you. *ProPublica*. https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you. Retrieved September 13, 2013, from http://www.propublica.org (originally published March 7, 2013).

46 Beckett, L. Everything we know about what data brokers know about you. *ProPublica*. https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you. Retrieved September 13, 2013, from http://www.propublica.org (originally published March 7, 2013). Singer, N. (2012, June 16). Mapping, and Sharing, the Consumer Genome. *The New York Times*. Retrieved at http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?_r=0).

47 https://isapps.acxiom.com/optout/optout.aspx; https://signup.euclidelements.com/optout.

Below is an example of the information that could be generated about Ruth by a data aggregation service cross referencing databases and making reasonable inferences from data collected.

1. Home address and phone numbers (mobile, home, work), when she purchased her house, the value of the house, amount of the mortgage, any liens and foreclosures, and insurance company.
2. Daily, weekly, and monthly patterns of arriving and leaving the house, sleeping patterns, preferences in house temperature, energy consumption, and what types of pets are in the house.
3. Age, race, gender, height, weight, hair color, unique physical characteristics, place of birth, and maybe her social security number.
4. Marital status, name of husband if married, names of past husbands, number of children and their ages, where the children go to school, friends of her children and where they live.
5. License plate number, make and model of car, emissions, mechanical problems, value of the car, any other information on the car registration, and car insurance company.
6. Credit history and information found in a credit report, including credit card numbers, credit limits, credit requests, salary and other income, missed payments, average, high, and low credit card balances.
7. Legal actions, including criminal convictions, maybe arrests, and any civil lawsuits.
8. Religious preferences, if any, and medical visits to clinics.
9. Travel routes, when and where tolls were paid, car speed, braking patterns, acceleration habits, traffic light and speed violations, miles driven, fuel efficiency, amount and type of gas purchased.
10. Her preferences in shopping locations (i.e., which malls and which stores in malls) and parking preferences which are reflected in how often she visits a mall and the stores in the mall and how much time she spends in the mall and stores, how she shops within stores, the amount of money spent at stores.
11. Preferences in clothing purchased on credit or at locations where she has been identified by facial recognition, including her responses to specific items in window displays, on mannequins, and in store displays; the amount of time she spent examining specific items and maybe her visual response to the item.
12. Preference in food purchased, including which types of food, quantity, calories, and frequency of purchase of similar food types.

13. Any public information found on Facebook, Google Plus, or other social media sites, including where she visits and places or things she "likes" on Facebook.
14. Any private information found on social media sites that mine pictures and text off members.
15. Interests based on her choice of affinity cards, such as airlines, gas, hotels, sports teams, or charities.

There will be less information about Tom because he is a minor, but some information could be collected about him as well:

1. Physical characteristics obtained by surveillance cameras, and maybe individual identification via facial recognition, including approximate age, race, gender, height, weight, hair color, unique marks.
2. Route taken through the mall and stores, mostly when accompanied by his mother, but if his phone collects this information, then personal information will be collected on his movements, including what stops he made, which items examined, and which items he purchased.
3. Tom's sizes and preferences in types of clothing brands, colors, and styles
4. Type of food that was purchased, items, quantity, calorie count per item, frequency of purchase of similar food types.
5. Tom's birthdate, gender, age, home address, email address.
6. Time Tom entered and left the mall and the parking garage, as well as when he left and arrived home.

Still believe that the details of your life go unnoticed? Does it bother you that so many aspects of your every day, personal life are being tracked, recorded, analyzed, and stored? Does this seem like an invasion of privacy to you, or do you welcome the advertisements and coupons? Would you change your daily lifestyle to avoid monitoring and act differently once you know you are being watched and tracked? Would you seek out ways to avoid this erosion of your personal privacy, such as wearing "personal camouflage" to hide your identity in public or glasses that "blind" surveillance cameras, and purchasing software that helps block digital intrusions?[48]

Despite our being aggressively monitored and profiled every day, only recently has there been a relatively widespread "call to arms" regarding personal privacy in this rapidly developing digital ecosystem. In the wake of revelations about extensive privacy intrusions, by both the government and the private sector, there have been repeated calls to expand personal privacy protections. For example, noting that companies are "monitoring your every move," the *New York Times* editorialized that we need laws setting "clear rules that would regulate and limit how businesses collect personal information, what they can use it for, and how long they keep it" and which would "give consumers an easy way to review files about themselves or simply choose not have the information collected."[49] The Federal Trade Commission and President Obama have also called for laws to protect consumer privacy, and Congress has introduced privacy bills, but there is no federal legislation to date.[50] However, given the powerful commerce and security interests involved, not to mention that some are untroubled about losing their privacy—at least, if they get discounts—this call to arms may go unheeded. One encouraging development is that some technology companies and privacy advocates have developed a voluntary Code of Conduct to regulate collecting "retail location analytics." Whether this code will be widely adopted or emulated in other monitoring and analytics domains remains to be seen.[51]

About the Authors

Gary L. Renz, PhD., JD, is a professor of management in the George Herbert Walker School of Business & Technology, Webster University in St. Louis, Missouri. He has taught courses in Human Resources Management, Organizational Behavior, Leadership, and Law. Dr. Renz earned his doctorate at the University of Minnesota and his law degree at UCLA. His current research interests focus on improving organizational performance and social networks. He may be reached at renzga@webster.edu.

Albert J. Marcella Jr., PhD, CISA, CISM, is president of Business Automation Consultants, LLC. Dr. Marcella is an internationally recognized public speaker, researcher, and workshop and seminar leader with 36 years of experience in IT audit, security, and assessing internal controls. He has authored numerous articles and 26 books on various IT, audit, and security related subjects. He can be reach at amarcella@mindspring.com.

48 Gallagher, R. (2013, January 18). These goofy-looking glasses could make you invisible to facial recognition technology. *Slate*. Retrieved from http://www.slate.com/blogs/future_tense/2013/01/18/isao_echizen_and_seiichi_gohshi_s_privacy_visor_shields_you_from_facial.html on November 23, 2013. Harvey, A. (2013, October 9). Camouflage from computer vision. *CV Dazzle*. Retrieved from http://cvdazzle.com/ on October 10, 2013. http://dismagazine.com/dystopia/evolved-lifestyles/8115/anti-surveillance-how-to-hide-from-machines/ retrieved on November 1, 2013. Harvey, A. (2012, December). Stealth Wear: New designs for countersurveillance. AH Projects. Retrieved from http://ahprojects.com/projects/stealth-wear on November 2, 2013. OFF Pocket is a smartphone holder that blocks wireless signals; https://offpocket.com/ retrieved on November 2, 2013.

49 Editorial (2013, October 9). Monitoring your every move. *The New York Times*. Retrieved from http://www.nytimes.com.

50 Federal Trade Commission Report, (2012, March). Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers. Retrieved from www.ftc.gov/os/2012/03/120326privacyreport.pdf. The White House, (2012). Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. Retrieved from www.whitehouse.gov/sites/default/files/privacy-final.pdf. See California's "Shine the Light" law at http://epic.org/privacy/profiling/sb27.html (retrieved December 30, 2013) for a state law on customer privacy.

51 http://blog.euclidelements.com/2013/10/senator-schumer-and-tech-companies.html. Schumer, C. E. (2013, October 22). Schumer, Tech companies and privacy leaders announce important agreement to ensure consumers have opportunity to "opt-out" before stores can track their movement via their cell phones—A practice that is becoming increasingly more common. Retrieved at http://www.schumer.senate.gov/record.cfm?id=346912&); http://euclidanalytics.com/privacy and https://signup.euclidelements.com/optout.