Digital Breadcrumbs: A Lack of Data Privacy and What People Are Doing About It

Carley Ward(✉), Dana Ellis, Lisa A. D'Ambrosio, and Joseph F. Coughlin

Massachusetts Institute of Technology AgeLab, Cambridge, MA, USA
carleyw@mit.edu

Abstract. With the seemingly ubiquitous presence of technology, interactions and transactions constantly take place over websites, apps, text, and email. Despite the convenience and efficiency of these modes of communication, these online interactions give many parties access to personal information and can leave individuals' information vulnerable to misuse and attack. As people use electronic devices for more and more tasks, they leave behind evidence of their activities, a trail of digital breadcrumbs providing behavioral and demographic information about where they go, whom they talk to, what they do, and what they believe. Consumers are often unaware of who has access to these data and how they might be used. In this mixed methods study, researchers conducted a series of surveys and focus groups in the United States to examine the everyday digital breadcrumb trail people leave behind when using technologies on a daily basis, people's awareness of this trail of data, and what measures they take to protect their digital information and prevent it from being collected or misused. Participants discussed their attitudes about data privacy, sharing, and trust. Implications for research, business, and policy are provided.

Keywords: Data privacy · Digital breadcrumbs · Mixed methods

1 Introduction

With the seemingly ubiquitous presence of technology, interactions and transactions constantly take place over websites, apps, text, and email. As of 2017, 77% of American adults owned a smartphone [1]. In one study of smartphone users, the average participant used their phone 76 separate times per day [2]. Despite the convenience and efficiency of these modes of communication, online interactions can leave individuals' information vulnerable to misuse and attack.

As people use electronic devices for more tasks, they leave behind evidence of their activities, a trail of digital breadcrumbs providing information about where they go, whom they talk to, and what they do. The fear of credit card information, transaction history, location history, home address, and email and bank account passwords being accessed or used unethically is not unjustified. In one study, 46% of smartphone users reported that they have had a company take advantage of their data and use it for something that they had not agreed to [3]. The present study examined the everyday digital breadcrumb trail people in the United States leave behind when using

M. Kurosu (Ed.): HCI 2018, LNCS 10901, pp. 599–612, 2018.
https://doi.org/10.1007/978-3-319-91238-7_46

technologies on a daily basis, people's awareness of this trail, and attitudes about data privacy, sharing, and trust.

2 Literature Review

2.1 Use of Technology and the Trail It Leaves Behind

As the technology business has boomed, people have come to use their computers, tablets, and smartphones for an increasing number of tasks. In a 2015 Pew Research Center study, smartphone owners in the US had used their phones in the past year to look up information about a health condition (62%), do online banking (57%), search real estate listings (44%), research information about a job (43%), look up government services or information (40%), and get educational content (30%) [1]. In addition, smartphone owners used their phone at least occasionally to follow breaking news (68%), share pictures or video about community events (67%), learn about community events (56%), get turn-by-turn navigation while driving (67%), and get public transit information (25%) [1]. Dscout (2016) reported that the average Android user touched their phone screen 2,617 times per day, with the most touches occurring on Facebook (15%), Messages (11%), the Home Screen (9%), and Chrome (5%) [2].

The Internet of Things provides abundant opportunities for convenience and connectivity, but it also creates new cybersecurity issues. The Internet of Things includes a variety of smart home or connected home devices including smart refrigerators, doorbell cameras, keyless locks, thermostats and smoke detectors, lights and blinds, and televisions. In one study, 90% of consumers cited personal or family safety as the top reason for smart home technology adoption [4]. The same study reported that 71% of consumers feared that their personal information may be stolen, and 64% feared that their data would be collected and sold [4]. These fears are not without warrant; most devices do not provide a secure mode of operation. In one study of 50 smart home devices, none of them enforced strong passwords, used mutual authentication (where individuals prove their identity to the server, and the server proves its identity to the individual), and almost 20% of apps used to control said devices did not encrypt communications to the cloud [5]. In 2014, hackers took advantage of these security gaps; there was a large-scale attack on smart home devices, including TVs and refrigerators, in which hackers were believed to have accessed more than 100,000 devices [6].

There are opportunities to collect data about the way people move about their communities as well. Drivers frequently pass cameras while driving, which record timestamps and license plate numbers. Additionally, many drivers encounter toll roads and use registered electronic toll passes. Similarly, many vehicles have built-in GPS which monitor drivers' progression on a route. Other drivers use smartphone navigation or map apps for directions. For example, the traffic and navigation app Waze collects and shares data with local governments [7]. Some cars collect and transmit data on driver speed, location, and braking. Tesla records video in their vehicles on the road to improve their autopilot system. Tesla's privacy policy states that they can share data with business partners, service providers, and other parties [8]. Outside of the car, public transit pass usage can be recorded, and some passes are registered with name and credit card information connected. Similarly, some public transit passengers use apps to identify transit arrival times, and some pedestrians use GPS or map apps to identify efficient walking directions.

In the context of health, digital data are collected on fitness trackers or other wearable devices (e.g., Fitbit). Organizations can use health data collected from fitness trackers and apps including location, activities, sleep patterns, biometric data, and reproductive health data for their own purposes [9]. For example, the Australian supermarket Coles encourages consumers using health trackers to link them to their loyalty cards by providing "loyalty points for walking 10000 steps per day" [9]. Insurance companies and employers may also see uses for health data.

All of these activities using electronic devices leave evidence behind. Most service providers, apps, and online companies collect and use the information people leave behind while using their product. For example, Facebook, which received the most touches of any app [2], records information from users' posts, messages, photos, videos, birthdays, relationship statuses, schools attended, hometowns, check-ins, and everything they have viewed, liked, or shared. Each touch is a decision which provides information about the user. Many more companies also require people to allow them access to other digital data in order to gain access to the product. For example, go to download the popular social media app Snapchat and a box will pop up to notifying the user that Snapchat requires access to in-app purchases, identity, contacts, location, SMS, photos/media/files, camera, microphone, Wi-Fi connection information, Bluetooth connection information, and device ID and call information. Accept?

2.2 Data Privacy or Lack Thereof

Privacy is an individual, group, or institutions' right to determine when, how and to what extent information about themselves is shared with others [10]. By engaging with online entities and accepting privacy agreements, individuals often unknowingly give up their right to privacy. Sixty percent of millennials report that they would be willing to share data about their preferences and behaviors with marketers, and 30% would be willing to provide even the most private data in return for discounts [11]. Not all age groups are equally willing to share their data, however. Only 13% of baby boomers would be willing to share private data in exchange for discounts. Additionally, 63% of US adults reported that they feel concerned about their privacy and security when they access the internet on their cell phones [3]. Likewise, 78% believe that it is difficult to trust companies when considering how they use consumer data and feel that service providers have too much information about consumer preferences and behaviors [12]. Only 44% of millennials believe companies they interact with keep their personal information private [13].

Once the apps, services, and websites collect user data, they are often able to give others access to these data. A study of apps in the US, Australia, Brazil, and Germany found that between 85% and 95% of free apps and 60% of paid ones connected to third parties that collected personal data [14]. In a study of 200,000 participants who visited 21 million web pages, third party trackers were present on 95% of those web pages [15].

Furthermore, retail, travel, media, telecommunications, and finance companies also collect and use digital data to develop products or services to improve marketing and sales and to personalize advertising and discounts. In addition to using these data for their own purposes, organizations frequently sell or share these data with other parties. Google (2017), for instance, reported that it captures "approximately 70% of credit and debit card transactions in the US" through third-party organizations [16]. Companies and data brokers use information such as demographics, credit history, medical history, and browser history to create profiles, which can be used for classification, estimation, or prediction [17]. Companies can use these profiles to target individuals with certain characteristics, influence behavior, predict their health risks or credit risk, or determine if they are desirable employees, good tenants, or valuable customers [18]. For example, US consumer reporting agencies provide reports to employers, landlords, insurance companies, and government agencies. Reports for employers may contain information about an individual's employment, salary, education, driving history, health, drug testing information, and fingerprints. Generally speaking, anyone can purchase lists of personal data of nearly every demographic. For example, ExactData.com has premade lists of "Americans with Bosnian Muslim Surnames" and "Unassimilated Hispanic Americans" [19].

Even when data are intended to be confidential and secure, hacking and stolen data are commonplace. For example, the data breach of the consumer credit reporting company Equifax, which began in May 2017 and continued until it was discovered in July, was not made public until September. Over the course of these two months, more than 145 million records were accessed, with information such as names, Social Security numbers, birth dates, addresses, driver's license numbers, credit card numbers, and certain dispute documents [20]. Further, Equifax experienced smaller breaches in 2016, 2012, 2010, and 2006 [20].

3 Methods

The present study examined the digital breadcrumbs that people leave behind, people's awareness of this trail, and attitudes about data privacy. Data were collected in two parts. First, we conducted a multipart survey (N = 36) mapping participants' technology use over a 24-h period, as well as collecting information on their technology adoption and use, methods they use to protect their data, and attitudes toward data privacy and sharing. Next, we conducted focus groups (N = 14) exploring what people know about the privacy of their data, how much they trust companies collecting digital data, and what factors come into play when deciding to use these companies.

3.1 Participants

Survey respondents were 36 (47.2% women) self-selected adults from across the US, ages 20–65 ($M = 42.9$), recruited from the MIT AgeLab Volunteer Database. Respondents were 83.3% White, 13.9% Asian, 2.8% Black, 2.8% Latino, and 2.8% other. Respondents ranged in technology savviness from 2.6 to 5 ($M = 3.9$) on a 1–5 scale where 5 indicated a high level of technology savviness. All respondents had at least some college education and over half of all participants (52.8%) had a total annual household income of at least $100,000 (see Table 1).

Table 1. Survey respondent demographics (N =36).

Category	Characteristics	Percent
Age	20–29	22.2
	30–39	25
	40–49	11.1
	50–59	22.2
	60–69	19.4
Gender	Men	52.8
	Women	47.2
Race	White	83.3
	Asian	13.9
	Black	2.8
	Latino	2.8
	Other	2.8
Education	Some college	11.1
	Trade/technical school or associates degree	2.8
	College Degree	22.2
	Some post-graduate work	16.7
	Post-graduate degree	47.2
Household income	Less than $25,000	13.9
	$25,000–$49,999	11.1
	$50,000–$74,999	13.9
	$75,000–$99,999	8.3
	$100,000–$149,999	22.2
	$150,000 or more	30.6

Focus group participants were 14 (71.4% women) Boston-metro area residents ages 23–59 (*M* = 48.9) recruited through local website postings. Participants' technology savviness scores ranged from 2.2 to 5 (*M* = 3.5).

3.2 Measures and Procedure

Surveys. Respondents completed a total of six online questionnaires over three days. The first questionnaire was an introductory survey with items about technology ownership and use (smartphone, cellphone, landline, computer, tablet, e-reader, GPS, credit or debit card, rewards or loyalty card, transit or toll pass, smartwatch, Fitbit or wearable, personal assistant device), smart home device ownership (smart thermostat, home security system, wireless doorbell camera, keyless entry, smart smoke/carbon monoxide detector, smart outlets/plugs, automatic lighting), and demographic information. Next, respondents completed one questionnaire every six hours over a 24-h period. These four surveys were identical and were used to document when respondents engaged in certain digital activities throughout the day, on which devices (smartphone, computer, tablet, smartwatch, and Amazon Alexa), using which software. Activities tracked included texting, social media use, making or receiving calls, email use, visiting websites, viewing maps, listening to music, reading, doing online banking, taking or viewing photos, video chatting, and online shopping. Finally, respondents completed a follow up survey exploring their attitudes, beliefs, and knowledge about data sharing, how they attempt to protect their data, and to what extent they trust in the companies and organizations that collect and use their data.

Focus Groups. Participants first completed a short online questionnaire providing information about demographics, technology savviness, and technology use. We conducted two focus groups over two days. Each focus group lasted two hours and included discussion led by two facilitators around the following topics: what kinds of data they believed were shared or vulnerable; what their data were being used for; what measures they took to protect their data; benefits and drawbacks of data sharing; attitudes about the sharing economy; and trust in organizations and brands. Focus groups were audio and video recorded.

4 Results

4.1 Technology Use and Data Sharing

Survey participants reported using their smartphones, computers, tablets, smartwatches, and smart thermostats throughout the 24-h data collection period (see Table 2). These devices were used for a variety of activities including texting, calls, social media, email, websites, maps, music, reading, banking, photos, video chatting and purchases. Smartphones were the most frequently used devices across time periods, with the most common activities being texting, social media, calls, visiting websites, and emails (see Table 3).

Table 2. The percentage of respondents who owned each device and who used each device in each time period.

Device	Sample percent (n)	Time period			
		12pm–6am	6am–12pm	12pm–6pm	6pm–12am
Smartphone	100(36)	36.1	86.1	88.9	80.6
Computer	94.4(34)	14.7	61.8	76.5	58.8
Tablet	50(18)	5.6	22.2	27.8	22.2
Thermostat	16.7(6)	16.6	16.6	33.3	16.6
Smartwatch	13.9(5)	20.0	20.0	20.0	20.0
Amazon Alexa	11.1(4)	0.0	25.0	0.0	25.0

Table 3. The percentage of respondents who used smartphones for each activity in each time period (N = 36).

Activity	Time period			
	12a–6am (n = 13)	6a–12pm (n = 31)	12p–6pm (n = 32)	6p–12am (n = 29)
Texts	53.8	83.9	96.9	82.8
Social media	30.8	45.1	56.3	51.7
Calls	0.0	54.8	68.8	41.4
Emails	38.5	71.0	56.3	44.8
Websites	46.2	64.5	31.3	37.9
Maps	7.7	32.3	21.9	17.2
Music	7.7	0.0	12.5	17.2
Reading	7.7	32.3	21.9	10.3
Banking	0.0	3.2	3.1	6.9
Photos	0.0	3.2	12.5	3.4
Video chat	0.0	0.0	3.1	3.4
Purchases	0.0	7.7	0.0	0.0

The constant use of these devices leaves an abundance of digital breadcrumbs with information about individuals' activities, locations, purchases, interests, and contacts; such information may be used by the company collecting it or sold to other companies. In addition to using personal electronic devices, respondents were sharing data while driving, taking public transportation, using rewards or loyalty cards, and making non-cash purchases (see Table 4).

Table 4. The percentage of respondents who engaged in each activity in each time period (N = 36).

Activity	Time period			
	12pm–6am	6am–12pm	12pm–6pm	6pm–12am
Driving	5.6	38.9	47.2	30.6
Public transit	0.0	5.6	2.8	5.6
Rewards card	0.0	13.9	13.9	2.8
Non-cash purchases	0.0	30.6	22.2	5.6

Similarly, most focus group participants reported using their cell phones constantly; as one 65-year-old man noted, "I never turn it off." One 25-year-old woman described herself as being on her phone "Most minutes of the day" for music, podcasts, and texting and using her tablet for watching Hulu and Netflix. Another (25-year-old woman) explained, "At least every hour of the day that I'm awake I'm using it [smartphone] in some capacity." A 39-year-old woman used her phone even when she was sleeping to play a white noise app from Spotify. Only three participants said that they were not constantly on their cell phones.

4.2 Beliefs About Data Sharing

Ninety-seven percent of survey respondents reported that they believed information about what they did online is collected, used, or viewed by others on a typical day. They believed that several different groups were collecting their digital breadcrumbs, including companies whose websites they visit, companies they purchase from, their internet provider, the US government, and hackers (see Table 5).

Table 5. Organizations which respondents believed to be collecting their digital data on a typical day (N = 36).

Organization	Percent
My internet service provider	77.8
Companies whose websites I visit	100
Companies I purchase from, have accounts with, subscribe to	94.4
Companies I don't purchase from, have accounts with, subscribe to	58.3
US Government	77.8
US Non-Governmental Organizations	52.8
Hackers	75.0

A majority of survey respondents reported that they believed many types of data were being collected about them, including their browsing history (100%), location (100%), purchase history (100%), email (97.2%), name (97.2%), social media activity (94.4%), IP address (88.9%), physical address (83.3%), phone number (83.3%), birthdate (80.6%), credit card information (69.4%), photos (66.7%), and passwords (61.1%).

Focus group participants also perceived that data about their digital behavior were being collected. Many made statements such as: "It's the new reality that everything is being tracked" (39-year-old woman); "Everything, literally everything [is being tracked]. Any possible way they can make money (39-year-old, woman); and "Everything [website] you visit is going to be collecting data on you" (23-year-old man). Participants listed many devices other than their smartphones that collected data on them throughout the day, including security cameras, Internet of Things devices, loyalty cards, GPS, cars, red light cameras, and credit or debit cards. A 39-year-old woman summed it up by saying, "I'm trying to think of where in modern life, if you're living in an urban area, where you could go where you're not being tracked."

Pros and Cons of Data Sharing. Survey respondents and focus group participants believed there were pros and cons to data sharing. Seventy-five percent of survey respondents said they felt that there were benefits to the collection and use of their digital data. The advantages they saw included helping companies develop better products and services, creating better website experiences, and receiving personalized information, such as customized ads, marketing campaigns and offers for things they might be more interested in purchasing. Further, many reported that they would feel comfortable with companies using their data if those companies offered them discounts for products and services (42%) or if it made things easier or more convenient (39%) (see Fig. 1).

IIn addition to these benefits, focus group participants discussed a variety of others. Many focused on the fact that data sharing offers convenience and saves them time and money. A 69-year-old woman in a focus group commented, “I started using Waze a few years ago even to go a few miles because it navigates you around the traffic. I tend to use it fairly frequently, and I guess I don’t mind the tracking that goes with it.” A 65-year-old man explained, “I guess it’s a small price to pay for the convenience that if I’m looking for something, I can find the lowest price and go buy it, rather than go to the store and go to another store and the time spent is unbelievable!” A 64-year-old woman added that companies would send her discounts for items that she had viewed on their websites, but had not purchased, so now when she does online shopping, she puts items in the cart, and then waits for an email with a coupon to arrive.

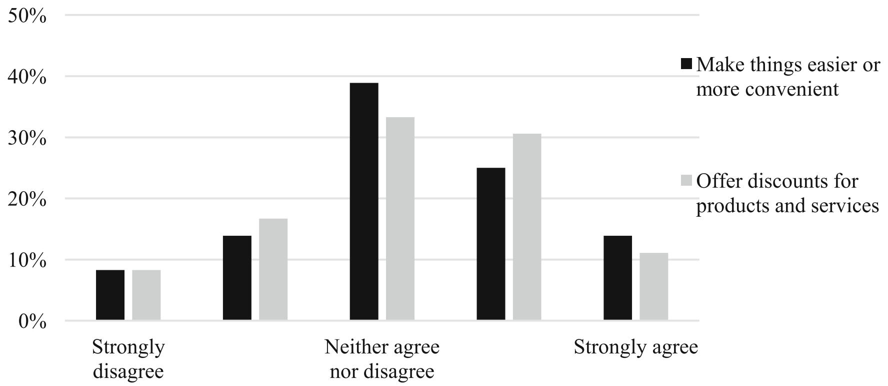

Fig. 1. Survey respondents: I would be comfortable with companies using my data if they (N = 36).

Focus group participants also identified a peace of mind that came with having the information that accompanies a digital transaction. One 26-year-old woman said, “If something bad happens in a cab or if I lose something in a cab, the chances of me ever being able to find that driver, to identify them, are pretty slim, whereas in an Uber you’re being tracked by GPS, you know the name and contact information of the driver right away”. The same theme was echoed around finances. Several participants remarked that because their banks and credit card companies track their spending patterns, they would automatically freeze participants’ accounts if any red flags occurred and call them to make sure their information had not been compromised. As one 39-year-old woman explained, “I know that my bank has my spending information, if that’s the protection that I’m gonna get, I’m comfortable with them having my information”.

In addition to personal benefits, one group discussed the societal benefits of collecting both individual and aggregated data. For example, a 65-year-old man mentioned how law enforcement and the legal system use evidence and the digital traces from electronic devices in criminal cases. He said, "I don't have a problem with it. In fact, sometimes I think it keeps us safer… I mean, unless I commit a crime, so what?" Another 50-year-old woman identified potential health benefits: "they can actually monitor disease progression and outbreaks by what people are googling and searching". She continued to note potential benefits around traffic flow, explaining how the Massachusetts Turnpike could determine the ideal time to schedule road construction based on EZPass data showing "when there's the fewest people using this particular stretch of road".

Despite the benefits identified, all of the survey respondents and focus group participants agreed that there were disadvantages to data sharing. Some of the disadvantages identified by survey participants included companies exploiting them for financial gain, fraud, risk of a breach of confidential information, identity theft, loss of privacy, and receiving junk advertising. Only 22.2% believed that companies used their data responsibly, and 86.1% believed that companies made money from their data. A majority reported that it was very or extremely important to protect their social security number (100%), passwords (100%), credit card information (100%), bank account information (100%), address (86.1%), phone number (75.0%), photos (75.0%), birthdate (69.5%), IP address (63.9%), purchase history (58.4%), and geographic location (55.6%).

Focus group participants also felt exploited or thought that having data constantly collected about them was creepy. One 39-year-old woman passionately exclaimed, "they're taking literally all of the information, every parameter they possibly can, and shooting it out any possible way they can to make money!" Others expressed discomfort with the fact that many privacy agreements allow companies, once they have collected data, to sell it to any number of other unidentified organizations. A 47-year-old man put it succinctly: "I feel like I'm being big brother-ed." A 69-year-old woman provided an example, "I was eating in some obscure restaurant, and then up came something, how did you enjoy your experience at this place, and I thought 'How do they know I'm here?' You know, that kind of thing is just creepy to me because I didn't put in that I was there, but it knew".

4.3 Data Security and Stolen Data Experiences

Focus group participants discussed using a range of methods to try to protect their information. Some reported using physical protections such as covering the keypad when entering their pin number or placing tape over their webcam. One 39-year-old woman said, "I have the tape right over it [webcam] and then when I saw the thing that said Zuckerberg has his microphone cut off somehow I was like ooh, how do I do that?" Others used process protections such as a VPN or private browsing, turning off location services on their devices, and creating strong passwords. One 23-year-old man said, "I'm careful what websites I go to avoid viruses. For example, I'll use a VPN if I'm on public wifi". Still others said they did not do anything. Participants who did not make efforts to protect their data either were not aware of what to do or felt their actions were futile. As one summed it up, "It's a crap shoot. If it's gonna get hacked, it's gonna get hacked" (65-year-old man).

Survey respondents were similarly not very intentional with data security. Twenty-five percent of respondents used a service to monitor fraud or identity theft. The majority changed their passwords only when a website required it (33.3%) or when they couldn't remember their password (27.8%), and most cleared their browsing history or internet cache on their phones if they happened to think of it (55.6%) or had never done so at all (16.7%). In addition, only 1.9% reported using a VPN sometimes or always when they connected to public wifi networks. However, nearly all respondents reported that it was extremely important to protect their passwords (91.7%), bank account information (88.9%), credit card information (88.9%), and social security number (83.3%). To this point, the majority of respondents did report taking a few common digital security measures such as using dual authentication methods (52.8%) and Spyware or anti-virus software on their computers (65.7%). They were much less likely to have Spyware or anti-virus protections on their phones (19.4%) or tablets (16.7%).

Stolen Data and Identity Theft. Unfortunately, having digital information stolen or misused is common. Many survey respondents reported having their email (44.4%), credit card (36.1%), or debit card (19.4%) information hacked, or even their identity stolen (22.2%). Overall trust in organizations to keep personal data secure was very low, with only 36.1% trusting companies they use, 30.5% trusting their internet service provider, 25.0% trusting the US government, and 11.1% trusting companies whose websites they visit. When asked to think about specific companies they used, however, reported trust was often much higher. A majority of respondents trusted their digital information with their bank (88.9%), credit card company (77.8%), healthcare provider (77.8%), home or auto insurance company (63.8%), pharmacy (58.3%), and Amazon.com (55.6%).

Nearly all focus group participants also reported their data had been compromised at least once through large data breaches, hacked ATMs, identity fraud, phone scams, or stolen credit cards. A 55-year-old man explained, "One time it was identified as BJ's Wholesale Club, another time it was TJX where there were massive breaches. You can get it stolen anywhere".

When asked how worried they felt about having their data stolen, focus group participants and survey respondents diverged. Fifty-three percent of survey respondents reported they were very worried about their personal information being stolen or hacked and 55% of said that they did not have control over what information they shared digitally. Interestingly, despite the frequency of the misuse of digital data, many focus group participants were not overly concerned about being hacked. In one group, when asked directly, *do you worry about being hacked*, not a single participant was more worried than "In the middle". Participants made statements such as "Can't waste your time worrying about it" and "No point in worrying, there's nothing you can do". Additionally, participants reported that they had not changed their purchasing or technology use habits since experiencing hacks. A 26-year-old woman who had fraudulent tax returns filed in her name said that subsequently "literally nothing has changed". This may be because when data are stolen, issues are often quickly resolved by other entities, namely banks and credit card companies. A 39-year-old woman concluded that “part of the reason why I don’t stress out about it anymore. is that banks seem to really be on top of it.”

5 Discussion and Conclusion

The present study examined the everyday digital interactions of people in the United States, their awareness of how data can be collected and used, and attitudes about data privacy, sharing, and trust. In review, people used electronic devices for tasks in a variety of domains all day and often through the night, leaving a long trail of data about their behaviors. Many knew that this phenomenon was occurring, and they were able to identify types of information being collected and some of the agents collecting said data. Individuals used a variety of methods to attempt to protect their data, but most measures were not used consistently or across devices, and there remained feelings of futility around these actions.

Respondents’ use of their smartphones mirrored that of participants in other studies, primarily using their devices for social connection and messaging, engaging most frequently with texts, calls, and email [1, 2]. While much research examines how we use our smartphones, this study sheds new light to how we use other devices, how these other devices (including computers, tablets, smartwatches, and other smart home technologies) add to the density of digital data disseminated, and how people sought to protect their personal data from being used for unknown purposes by unknown agents.

As technologies continue to evolve and become ever more sophisticated, a tradeoff for the convenience and connectivity such electronic devices offer often means sharing data with other parties, resulting in decreased privacy and increased risks for individuals. These risks are not simply due to the exposure of financial data; adoption rates of smart home devices, fitness trackers, and other electronics that track everyday behaviors are on the rise. In 2016 there were 5.4 million multifunction or whole smart home systems in homes in North America [21], 72% of North Americans were Facebook users [22], and 10% of Americans owned a fitness tracker [23]. As technologies that can track individual actions and behaviors become ubiquitous, it is increasingly important that people be aware of the extent to which their every action is collected and shared, by whom and with whom, so that they can make informed decisions about whether and how they protect their data. It may be difficult to persuade individuals to adopt security measures if they believe that their efforts do not substantially lower the likelihood of their data being accessed or misused – even though there may be risks around allowing others to collect information about them. In particular, in the US, where data privacy laws tend to be less stringent than those in the EU, public educational campaigns or school curricula about personal data collection by third parties and types of precautions individuals could be taking to protect themselves could be crucial. Although participants in the present study were aware that their data were easily accessible and being collected by many parties, they primarily focused on how it was being used for advertising, shopping, and credit card fraud. Understanding the specific uses of their data and the consequences they have, now or in the future, may encourage individuals to be more attentive to their data security.

Acknowledgment. The authors gratefully acknowledge research support from Liberty Mutual.

References

1. Smith, A.: Record shares of Americans now own smartphones, have home broadband (2017). http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/
2. Dscout Mobile touches: Dscout's inaugural study on humans and their tech (2016). https://blog.dscout.com/mobile-touches
3. Husson, T., Khatibloo, F.: How will people trust you? Technical report (2015). https://www.forrester.com/report/How+Will+People+Trust+You/-/E-RES117920
4. Icontrol Networks 2015 State of the Smart Home Report. Technical report (2015). https://www.slideshare.net/iangertler/2015-state-of-the
5. Barcena, M.B., Wueest, C.: Security response: Insecurity in the internet of things (2015). https://www.symantec.com/content/dam/symantec/docs/white-papers/insecurity-in-the-internet-of-things-en.pdf
6. Marketwatch: Proofpoint uncovers internet of things (IOT) cyberattack. Marketwatch (2014). https://www.marketwatch.com/story/proofpoint-uncovers-internet-of-things-iot-cyberattack-2014-01-16?reflink=MW_news_stmp
7. Olson, P.: Why Google's Waze is trading user data with local governments. Forbes (2014). https://www.forbes.com/sites/parmyolson/2014/07/07/why-google-waze-helps-local-governments-track-its-users/#184a3f9339ba
8. Lambert, F.: Telsa updates data sharing policy to include collecting video in order to 'make self-driving a reality' (2017). https://electrek.co/2017/05/06/tesla-data-sharing-policy-collecting-video-self-driving/
9. Pingo, Z., Narayan, B.: When personal data becomes open data: an exploration of lifelogging, user privacy, and implications for privacy literacy. In: Morishima, A., Rauber, A., Liew, C.L. (eds.) ICADL 2016. LNCS, vol. 10075, pp. 3–9. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-49304-6_1
10. Westin, A.F.: Privacy and Freedom. Athenaeum, New York (1967)
11. Mintel: Sixty percent of millennials willing to share personal info with brands (2014). http://www.mintel.com/press-centre/social-and-lifestyle/millennials-share-personal-info
12. Loudhouse: The future of digital trust: A European study on the nature of consumer trust and personal data (2014). https://www.orange.com/en/content/download/21358/412063/version/5/file/Orange+Future+of+Digital+Trust+Report.pdf
13. Fleming, J., Adkins, A.: Data security: Not a big concern for millennials (2014). http://news.gallup.com/businessjournal/192401/data-security-not-big-concern-millennials.aspx
14. Seneviratne, S., Kolamunna, K., Seneviratne, A.: Short: a measurement study of tracking in paid mobile applications. In: Proceedings of the 8th AMC Conference on Security and Privacy in Wireless and Mobile Networks, New York, USA (2015). https://doi.org/10.1145/2766498.2766523
15. Yu, Z., Macbeth, S., Modi, K., Pujol, J.M.: Tracking the trackers. In: Proceedings of the 25th International Conference on World Wide Web (WWW 2016). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, Switzerland, pp. 121–132 (2016)
16. Google: Powering ads and analytics innovation with machine learning (2017). https://adwords.googleblog.com/2017/05/powering-ads-and-analytics-innovations.html
17. Berry, M.J.A., Linoff, G.S.: Data Mining Techniques: For Marketing, Sales, and Customer Relationship Management, 2nd edn. Wiley Publishing, Indianapolis (2004)

18. Citron, D.K., Pasquale, F.A.: The scored society: Due process for automated predictions. WASH LAW REV, vol. 89, p. 1 (2014). https://ssrn.com/abstract=2376209. U of Maryland Legal Studies Research Paper No. 2014-8
19. O'Carroll, T., Franco, J.: Why build a Muslim registry when you can buy it? Amnesty Global Insights (2017). https://medium.com/amnesty-insights/data-brokers-data-analytics-muslim-registries-human-rights-73cd5232ed19
20. Equifax: Consumer Notice: Notice of Data Breach (2017). https://www.equifaxsecurity2017.com/consumer-notice/
21. Statista: Smart Home. Technical report (2017b). https://www.statista.com/study/27165/smart-homes-statista-dossier/
22. Statista: Facebook. Technical report (2017a). https://www.statista.com/study/9711/facebook-statista-dossier/
23. Statista: Wearable Devices. Technical report (2017c). https://www.statista.com/study/15607/wearable-technology-statista-dossier/