Consumer Perceptions of Privacy in the Internet of Things

What Brands Can Learn from a Concerned Citizenry

June 2015

By Jessica Groopman with Susan Etlinger

A research report based on a survey of 2062 American consumers

ALTIMETER®

The digitalization of our physical world—what many are now calling the 'Internet of Things'—is challenging our expectations of privacy.

Adding sensors to ourselves, and to the objects and places around us, renders our physical world communicable, contextual, and trackable. The full implications of ubiquitous connectivity remain blurry, but Altimeter Group's survey of 2,062 American consumers makes one point crystal clear: Consumers are decidedly anxious about how companies use and share data from their connected devices. Our research finds a massive gulf between consumer awareness and industry practices when it comes to privacy. But this data reveals more than a concerned citizenry, it reveals tremendous opportunities for companies to foster more trusted customer relationships.

Key Findings:

1. Consumers' top concern: Who is seeing my data?

   Consumers are highly anxious about companies sharing their data: 78% of consumers highly concerned about companies selling their data to third parties.

2. At least half of consumers expressed extreme discomfort with the use and sale of their data in connected 'real world' environments.

   While older generations show higher concern, strong discomfort with the use and sale of connected device data is pervasive across all age groups, including millennials.

3. Consumers want more information and more engagement around privacy

   While trust and understanding of standard data collection and privacy protections are low, consumers are highly interested in deeper information and more frequent notifications.

4. Consumers demand value in exchange for their data

   Primarily in monetary form, but also in the form of time, energy, and convenience

5. Technological awareness informs trust and influences consumer expectations for engagement.

   Exposure to technology is a key indicator for expectations around notifications, service, communications, and trust.

Table of Contents

INTRODUCTION

When it comes to the mobility of technology and data use, the notions of controlling, revealing, and concealing our privacy shift. In the laptop era, our connection to the Internet was deliberate, optional, autonomous, and consensual; a matter of powering up a computing device, or shutting the laptop and walking away.

Enter the ambient data collection of sensors all around us. As sensors pervade our physical environments—the smartphones in our pockets, the appliances in our homes, the cars we drive, the stores we shop at, even the parks and street crossings we traverse— the potential (the inevitability) of passing through others' spheres of information gathering increases exponentially. In the Internet of Things, there is no shutting the laptop and walking away. As consumer interactions with digital technology shift from the desktop/laptop into the physical world, so must commercial messaging and transparency around these interactions.

Altimeter Group conducted a survey of 2,062 American consumers[1] to ascertain consumer perceptions of privacy around the Internet of Things. This report summarizes findings and insights from this data in an effort to address the unprecedented implication and challenge of the Internet of Things: privacy.

SUCCESS IN CONSUMER-FACING IoT DEPENDS ON ADDRESSING THE ELEPHANT IN THE ROOM

Any company seeking to apply IoT to consumer-facing programs long-term, and at scale must take a sober look at how consumers, *people* actually feel about adopting such technologies. For example:

- Recent data from Nielsen finds that 53% of Americans claim their top concern around IoT is that their data may be used or shared without their knowledge or approval.[2]
- Privacy, what it is (or is no longer), what agency we still have (if any) is another major concern consumers have around IoT. A recent survey by Ipsos and TrustE found that 42% of Americans are more concerned about their digital privacy than they were just 12 months ago.[3]

In the era of Edward Snowden, Wikileaks, numerous data and security breaches, consumer confidence in digital privacy is understandably low.

As an industry, why should we care? Trust isn't just bad for a company's image; it's a business risk, with a monetary value. A recent survey by Harris Interactive (on behalf of TRUSTe) found that nine out of ten consumers avoid doing business with companies who they feel are not protecting their privacy online.[4] To realize the many potential benefits IoT can offer, the industry must rethink its role in managing and messaging the risks of data as currency.[5] As data transforms business models, and devices transform customer experiences, so too must companies transform the manner in which they communicate both.[6]

What follows is a summary of findings from our survey aimed at addressing the key issues and opportunities consumer-facing brands must consider.

I. EXPOSURE TO IoT (OR LACK THEREOF) WILL IMPACT ENGAGEMENT

An important starting point to understanding how consumers perceive their privacy today is to look at exposure: exposure to connected devices, to the concept of the Internet of Things, and to existing templates for safeguarding, understanding, and accessing data.

MOST PEOPLE DON'T KNOW WHAT THE INTERNET OF THINGS IS

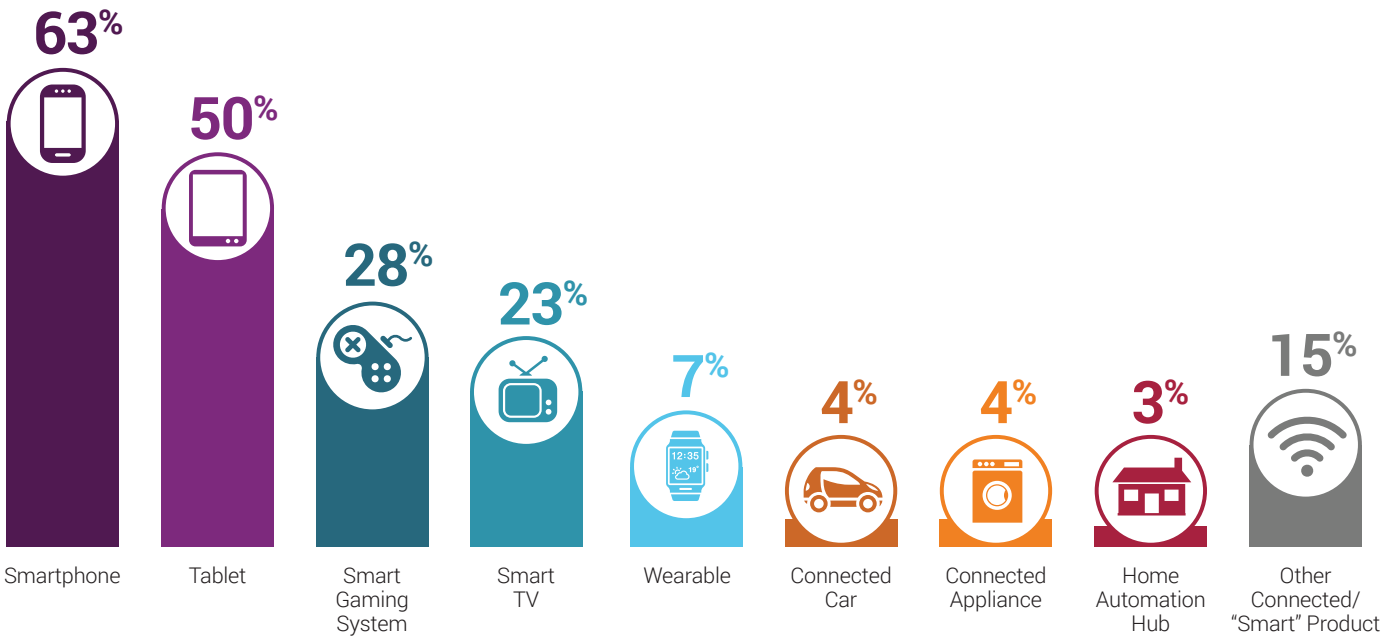
Understanding consumer perceptions of privacy in the Internet of Things begins with a reality check that most people don't know what the Internet of Things is in the first place. A recent study by Acquity Group found that 87% of consumers surveyed had never heard of the Internet of Things.[7] To the extent consumers are aware of IoT (which is limited—this same survey found 64% of respondents were unaware of the Nest thermostat), they are more familiar with connected objects in specific contexts. In other words, they might not know what IoT is, but they have a Fitbit for fitness tracking, have heard of autonomous vehicles, or perhaps have browsed the 'connected home' section at Best Buy.

This is important for two key reasons. One, it implies that 'IoT' is an industry term, used by the industry that powers it—not by the users it directly impacts. Two, it suggests consumer understanding is limited to the vertical (industry-specific) level, yet IoT is inherently a horizontal concept (i.e. it spans across multiple industries through partnerships, APIs, data sales, etc.). By extension, the data generated by IoT that impacts consumer privacy also spans across multiple industries.

In surveying the American public, we intended to gain a realistic snapshot of how consumers relate to connected devices; meaning respondents represented a spectrum of exposure to, adoption of, and familiarity with technology.[8]

FIGURE 1 CONSUMER ADOPTION OF IOT DEVICES UNDERWAY IN 2015

Q. Which of the following things (e.g. devices, objects) do you own today that connect to the internet?



Note: Data shown includes only connected mobile devices and connected objects; it does not include percentages of desktops and laptops.

Source: Consumer Perceptions of Privacy in the Internet of Things, Altimeter Group, 2015 Base: n=2062 respondents

87% of consumers surveyed had never heard of the Internet of Things

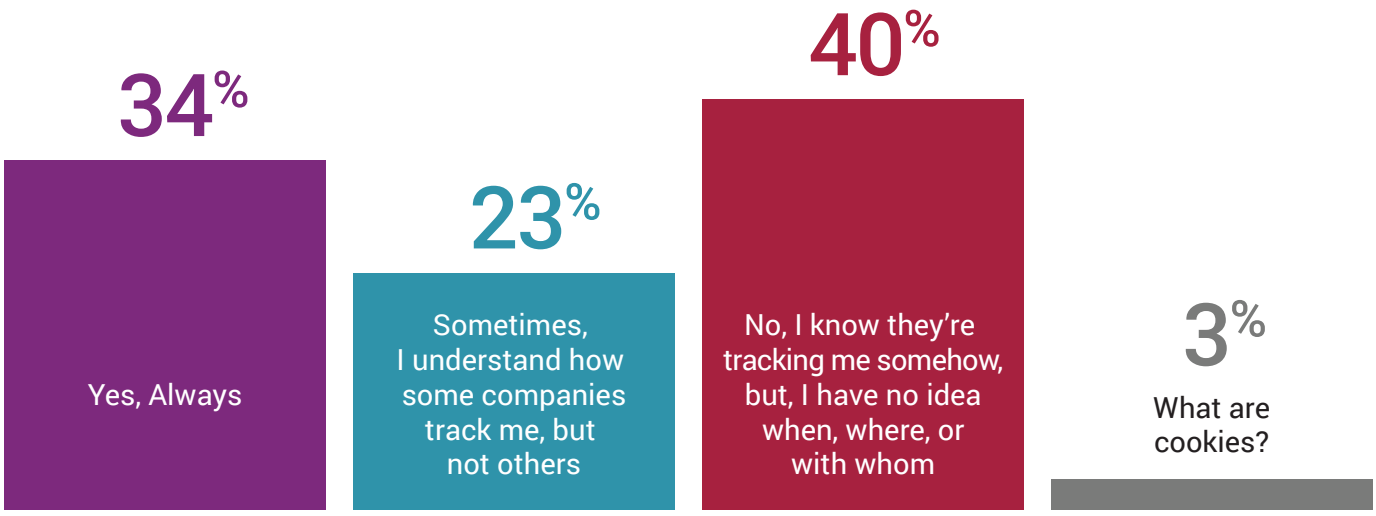
While consumers may not know what the Internet of Things is, the adoption of smart technologies is well underway. Indeed, most Americans have IoT devices in their pockets already: smartphones. Today, some 75% of Americans are walking around equipped with between 7-14 sensors transmitting information from their person.[9] Altimeter's study found some 70% of respondents owned a connected device other than, or in addition to, a smartphone, tablet, or laptop. That said, consumers are early in the adoption of many devices; 87% surveyed currently owned three or fewer connected devices. Forecasts from numerous research and technology institutions expect this number to increase to 7-26 devices per person by 2020.[10] Still, consumer understanding of IoT as a term, nevermind a phenomenon, is extremely low. To understand that a device is connected is not the same as understanding the implications of a connected ecosystem—of the Internet of Things.

IT'S NOT JUST FUTURE TECHNOLOGY, CURRENT TRACKING TECHNOLOGY IS STILL UNCLEAR TO USERS

It's not just emerging technology for which the larger American population lacks deeper awareness. This survey polled respondents on their awareness of 'cookies,' the default for online web browser tracking—a technology some twenty years in use.

FIGURE 2 TWENTY YEARS LATER, MAJORITY OF CONSUMERS STILL DON'T FULLY UNDERSTAND ONLINE COOKIES

Q. Are you aware whether or not specific companies with which you interact are tracking your 'cookies'?



Source: Consumer Perceptions of Privacy in the Internet of Things, Altimeter Group, 2015 Base: n=2062 respondents

Despite twenty years of cookie tracking on two channels (i.e. desktop and laptop), 40% of consumers don't understand how, when, where, or with whom this tracking occurs. When we asked the 23% of respondents (those who answered 'Sometimes') how they understood some companies were tracking them, but not others, responses indicate people are paying attention, perhaps more than brands think.

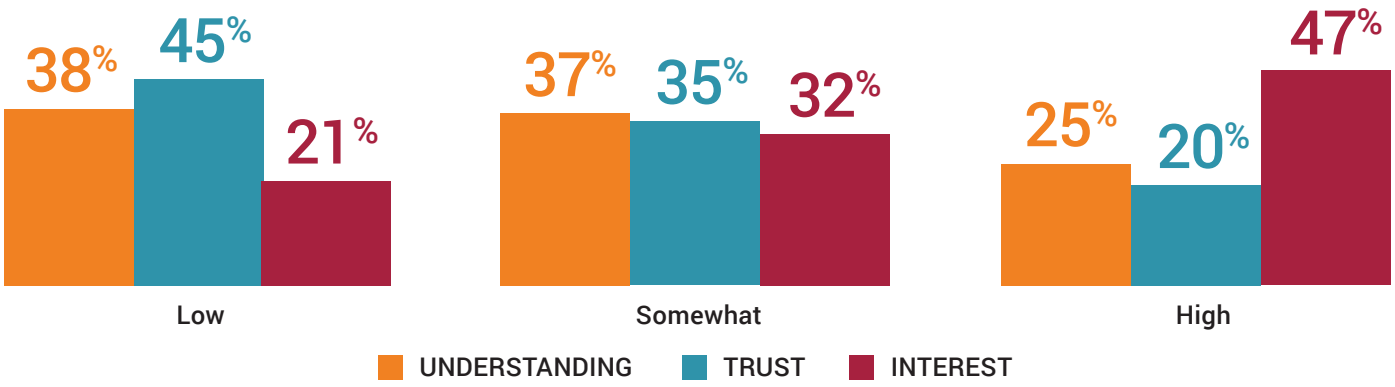

"I think different companies are tracking cookies differently which is worrisome. I wish there was consistency in tracking to make it easier to understand."
"It's more clear to me that my cookies are associated with each website. It's less clear to me what they use my information to actually accomplish."
"I see purposeful obfuscation and lack of transparency on the part of companies. Understanding is easier when a company is interested in telling me what they are doing with my data first, then interested in making a profit second."
"Some companies try to hide or bury their data usage in dozens of pages of documents you'd really have to dig into to find. Other companies are pretty up front in the first page saying what they will do with your data."

HIGHER EXPOSURE TO CONNECTED TECHNOLOGIES TRANSLATES TO HIGHER BRAND ENGAGEMENT

It may not come as a surprise that when we asked consumers to rate their level of understanding of how companies were using their data, three quarters did not feel confident. This study also finds that trust levels are generally low, with some 45% of respondents expressing very low trust or no trust at all that companies were using their connected device data securely and in ways that protected their privacy. Yet, while understanding and trust trend low, consumer interest in how companies are using such data is high. Almost half of all respondents claim they are very or extremely interested in learning more about how companies are using and protecting their data.

45%
of respondents express very low trust or no trust at all that companies were using their connected device data securely and in ways that protected their privacy

FIGURE 3A UNDERSTANDING AND TRUST IN HOW COMPANIES USE CONNECTED DEVICE DATA TREND LOW, INTEREST HIGH



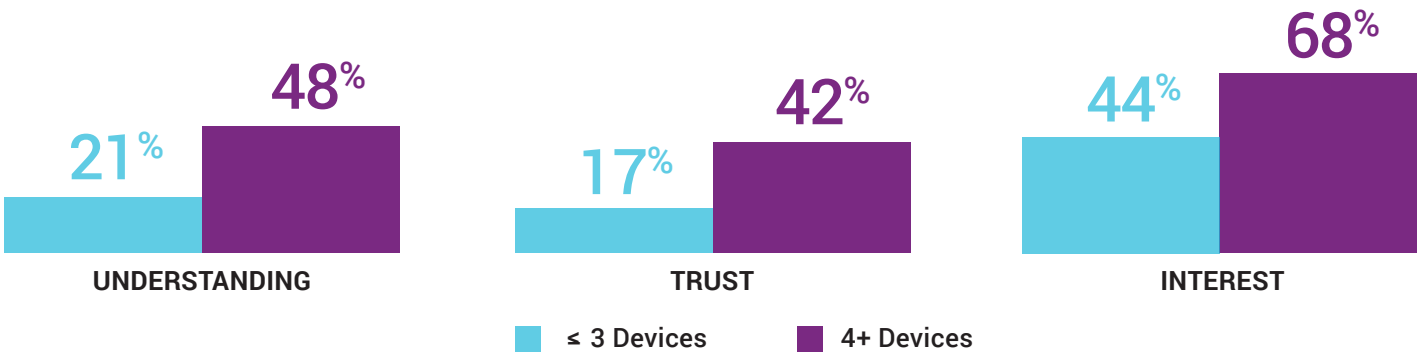
- How much of an **UNDERSTANDING** do you feel you have today about how companies are using your data from these connected things?
- How much do you **TRUST** companies are using your data from these connected things securely and in ways that protect your privacy?
- How much **INTEREST** do you have in understanding how companies are using data from these connected things?

Note: Respondents were asked to rate their understanding, trust, and interest on scale of 1-5 where 1 is was extremely low and 5 was extremely high.

Source: Consumer Perceptions of Privacy in the Internet of Things, Altimeter Group, 2015 Base: n=2062 respondents

FIGURE 3B CONSUMERS WITH GREATER EXPOSURE TO TECHNOLOGY REPORT GREATER UNDERSTANDING, TRUST, AND INTEREST IN HOW COMPANIES USE THEIR DATA

Q. Indicate your level of understanding, trust, and interest on a scale of 1-5 (chart shows percentage of 4's and 5's only)



Note: This chart breaks respondents into two groups (those with 3 or fewer connected devices vs. those with 4 or more connected devices). The percentages shown reflect the number of respondents (per group) who answered 'high or very high' (4 or 5) when asked the following questions:

Q. How much INTEREST do you have in understanding how companies are using data from these connected things?
(Rate on a scale of 1-5 where 1 not interested at all and 5 extremely interested.)

Q. How much do you TRUST companies are using your data from these connected things securely and in ways that protect your privacy?
(Rate on a scale of 1-5 where 1 is no trust at all and 5 is full trust.)

Q. How much of an UNDERSTANDING do you feel you have today about how companies are using your data from these connected things?
(Rate on a scale of 1-5 where 1 is no understanding at all and 5 is complete understanding.)

Source: Consumer Perceptions of Privacy in the Internet of Things, Altimeter Group, 2015

This study also finds that a consumer's exposure to technology is an indication of their level of engagement in the use of their connected device data. 'Engagement' can mean many things of course— [technological or brand] adoption, acceptance, understanding, trust, interest, interactions, desire for more interactions, etc. When we segmented data by the level of exposure consumers have to connected devices (number of devices owned), their levels of understanding, trust, and interest increase across the board. Those respondents with 4 or more connected devices ("High Exposure" respondents) report substantially higher understanding, trust, and interest in how companies are using their connected device data. (see Figure 3b)

Respondents with higher 'exposure' to technology have different expectations around how companies should interact with them. Trends illustrating these expectations weren't just a function of number of devices owned, but of living environment (urban vs. rural) as well as age. These expectations are characterized by a generally higher interest in engagement; in the depth, notification type, channel, and frequency of messaging as well as what constitutes 'value' when exchanging with a brand.

Respondents with higher 'exposure' to technology have different expectations around how companies should interact with them.

II. TREMENDOUS CONCERN OVER THE USE AND SHARING OF CONNECTED DEVICE DATA HIGHLIGHTS THE TOP BARRIER FACING IoT

In the most basic sense, the key difference between the Internet as it exists on a desktop, laptop or web browser versus the Internet of Things is that the latter implies a location-based context. Whether mobile device, object, or environment-based, sensors (and their ability to communicate with each other and the cloud) fundamentally change our relationship to the Internet, and the Internet's relationship to us.

CONSUMERS EXTREMELY UNCOMFORTABLE WITH USAGE AND SALE OF THEIR DATA ACROSS ALL PHYSICAL REALMS

As the Internet reaches into physical spaces—our stores, our cars, our homes, even our bodies— we must revisit the notion of privacy and our comfort with how various entities wield our data for commercial purposes. Altimeter's survey asked consumers to rate their level of comfort with how companies use versus sell their data, *assuming they (consumers) have opted in to their products and services*, across seven core domains we all traverse in our daily lives.

a.	On or related to our bodies (e.g. wearables, fitness trackers)
b.	In our homes (e.g. connected home products)
c.	In modes of private transportation (e.g. our cars, bikes)
d.	In modes of public transportation (e.g. our trains, planes)
e.	In public marketplaces (e.g. malls, in-stores)
f.	In public institutions (e.g. museums, stadiums)
g.	In public spaces (e.g. parks, street crossings)

Altimeter data suggest significant concern across all physical spaces, with more than 45% of all respondents they are "very or extremely uncomfortable" with companies using their data. Across the board (i.e. age groups, device exposure, environment, male/female), we also find people are significantly less comfortable with companies selling their data than they are with companies using their data. Roughly 60% of all respondents report such heightened discomfort in the sharing/selling of their data (See figure 4).

Areas of highest concern are:

- Our Bodies: More than 52% of respondents are uncomfortable or not comfortable at all with their data being USED in relation to their BODIES
- Public Spaces: Some 60% surveyed are uncomfortable or not comfortable at all with their data being SOLD or shared in PUBLIC SPACES

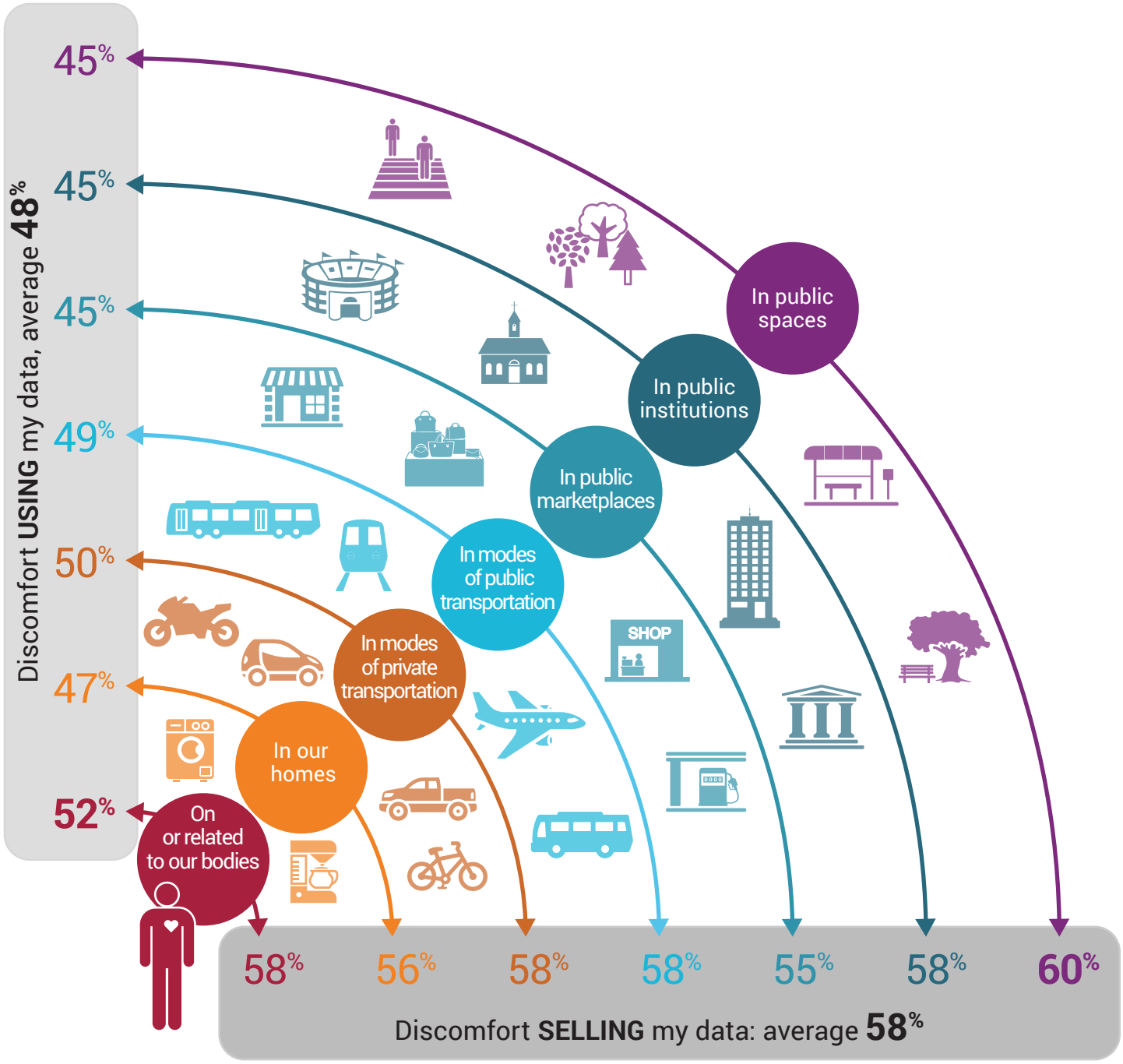
Areas of highest sensitivity suggest an imperative for companies to articulate and notify consumers of their intended use cases for consumer data.

Data suggest all physical spaces engender a sense of great discomfort when it comes to commercial use and sales of our data (even when opt-in is assumed). Across the population surveyed, 21% answered "extremely uncomfortable" (1) across every single domain.

This is even more pronounced with those who have lower exposure to technology; in this segment, approximately 50% selected "extremely uncomfortable" (1) with data selling across any physical space. Environmental and age differences also show variance, with the rural segment and more senior segments reporting higher discomfort with data use and sales than the general population.

FIGURE 4 ROUGHLY HALF OF ALL CONSUMERS HIGHLY UNCOMFORTABLE WITH COMPANIES USING AND SELLING THEIR DATA IN PHYSICAL SPACES

Q. How comfortable are you with companies USING vs. SELLING your data in each of the following areas, assuming you have opted-in to their products/services.



Note: These percentages reflect all respondents who, on a scale of 1-5 rated their comfort level as a 1 (extremely uncomfortable) or 2 (uncomfortable) with companies using vs. selling their data across each physical space.

Source: Consumer Perceptions of Privacy in the Internet of Things, Altimeter Group, 2015 Base: n=2062 respondents

CONSUMERS REPORT EMBEDDED SENSORS CALL FOR EXPLICIT MESSAGING

Areas where consumers expressed highest concerns around commercial use and sales of data may well indicate the desire for notification, as consumers' concerns around data use and sharing are similarly rated (in both percentage of 4's and 5's as well as ranking) to how they perceive the importance of notification. (See figure 5)

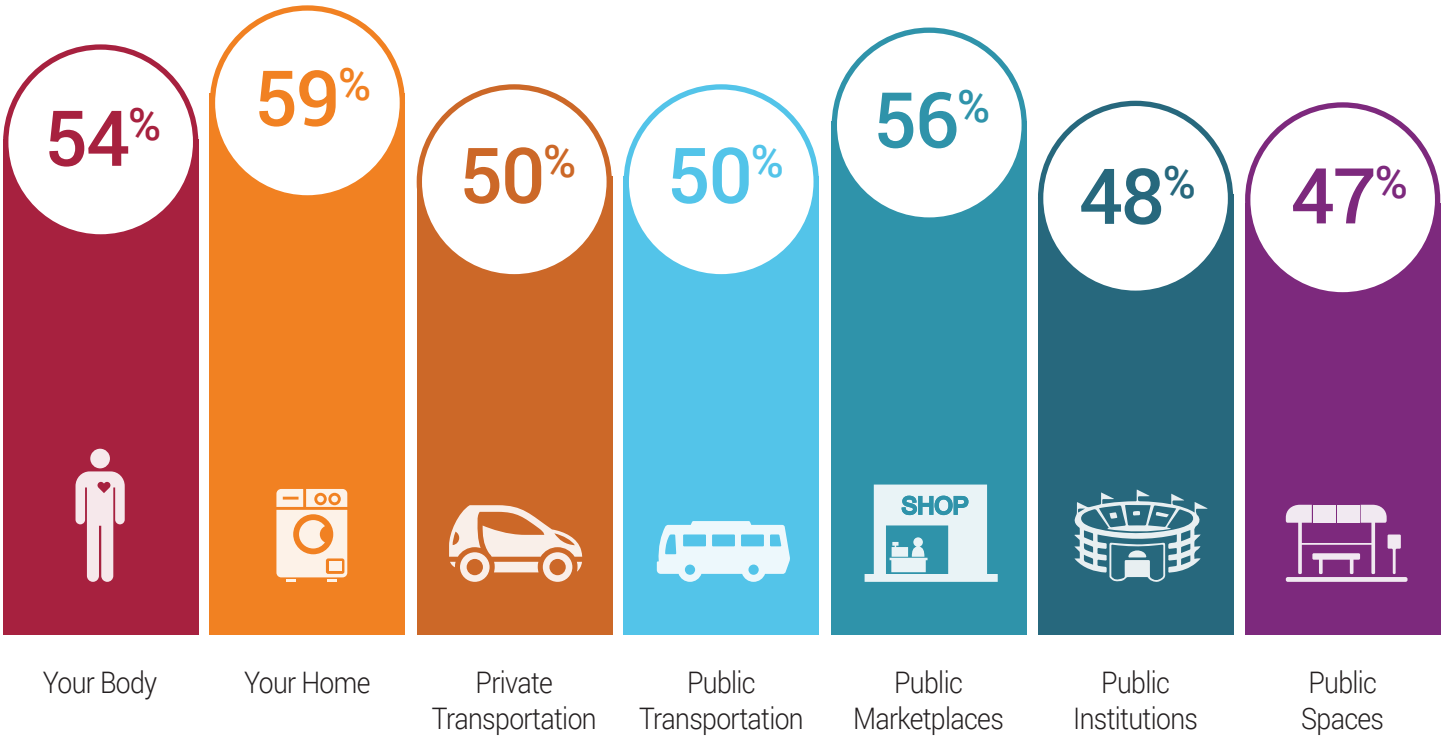
Areas of highest importance of notifications mirror those where consumers expressed the highest concerns around commercial use and sales of their data. Indeed these concerns may well indicate the desire for notification, as consumers' concerns around data use and sharing are similarly rated (in both percentage of 4's and 5's as well as ranking) to how they perceive the importance of notification.

Data from a recent Pew study validates the importance of notification. The study of 498 Americans found that people are averse to being observed without their approval:[11]

- 88% say it is important that they not have someone watch or listen to them without their permission.
- 63% feel it is important to be able to "go around in public without always being identified."

FIGURE 5 CONSUMERS PLACE HIGH IMPORTANCE ON NOTIFICATION OF DATA COLLECTION ACROSS ALL CONNECTED PHYSICAL SPACES

Q. How important is it to you for companies to NOTIFY you when they are collecting your data to provide you real-time services/offers?



Note: These percentages reflect respondents who rated the importance of notification as a 4 (important) or 5 (extremely important), out of a scale of 1-5 where 1 is not important at all and 5 is extremely important)

Source: Consumer Perceptions of Privacy in the Internet of Things, Altimeter Group, 2015 Base: n=2062 respondents

IT'S NOT JUST 'WHERE' THAT'S CONCERNING; CONSUMERS EXPRESS EXTREME CONCERNS ABOUT HOW COMPANIES ARE USING THEIR DATA

With more sensors follow more devices, which gives way to more varied manner in which companies can use and aggregate consumer data. This survey asked consumers to rate their privacy concerns across each of the following ways companies can interact with their data. The data suggest heightened privacy concerns center around three areas:

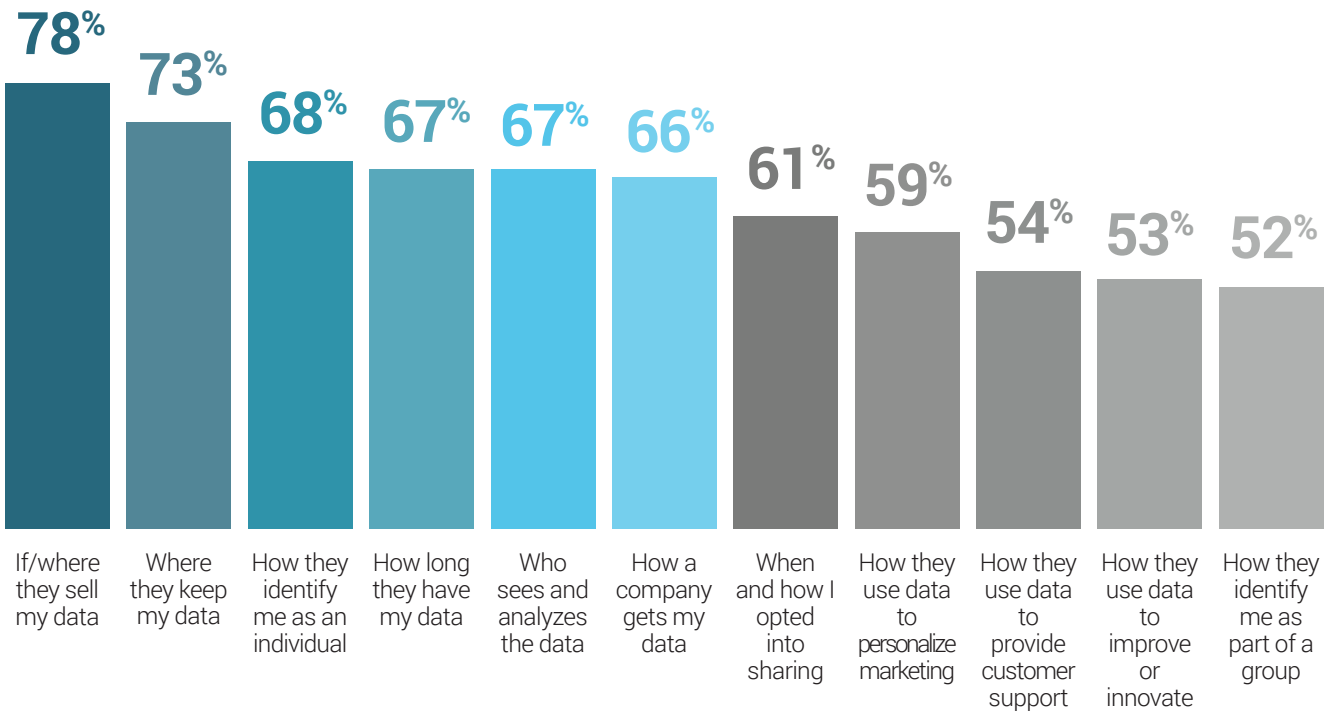
- Where and to whom my data is sold or exposed
- Where and how long my data is stored
- How personally (individually) identifiable data is

Across the general population, respondents voiced significant concern—over 50% report they are very or extremely concerned with companies using their data across all categories (See figure 6a). One out of five surveyed report extreme concern (a score of 5) in every single area.

As in the previous chart, concerns around selling and sharing data are generally higher than data usage. Some 78% of the general population are highly concerned about if and where companies are selling their data, and amongst the senior segment, this number jumps to 89%.

FIGURE 6A CONSUMERS' TOP PRIVACY CONCERNS ARE DATA SELLING, STORAGE, ACCESS, AND THE ABILITY TO BE IDENTIFIED INDIVIDUALLY

Q. Rate your level of privacy concerns across each of the following ways companies interact with your data.



Note: These percentages reflect all respondents who, on a scale of 1-5 rated their concern as a 5 (extremely concerned) or 4 (very concerned) with each of the ways companies interact with their data.

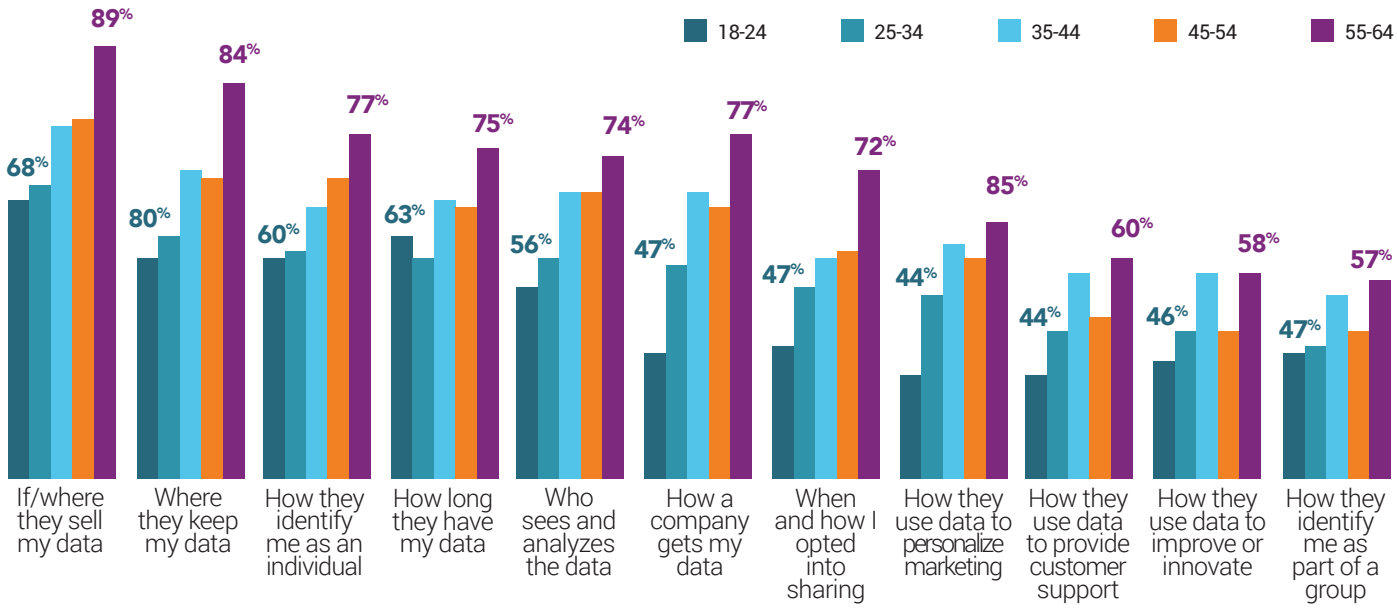
Source: Consumer Perceptions of Privacy in the Internet of Things, Altimeter Group, 2015 Base: n=2062 respondents

SENSITIVITY TO DATA USE IS NOT EXCLUSIVE TO OLDER POPULATION

While this data found substantially higher concerns about privacy from more senior age groups, this is not to imply that younger age groups 'don't care.' The chart below shows the level of privacy concerns related to data broken out across age groups. Even for the youngest segment, well over 40% indicated concern or extreme concern for each type of data use (See figure 6b).

FIGURE 6B OLDER SEGMENTS EXPRESS MORE EXTREME CONCERNS AROUND DATA PRIVACY

Q. Rate your level of privacy concerns across each of the following ways companies interact with your data.

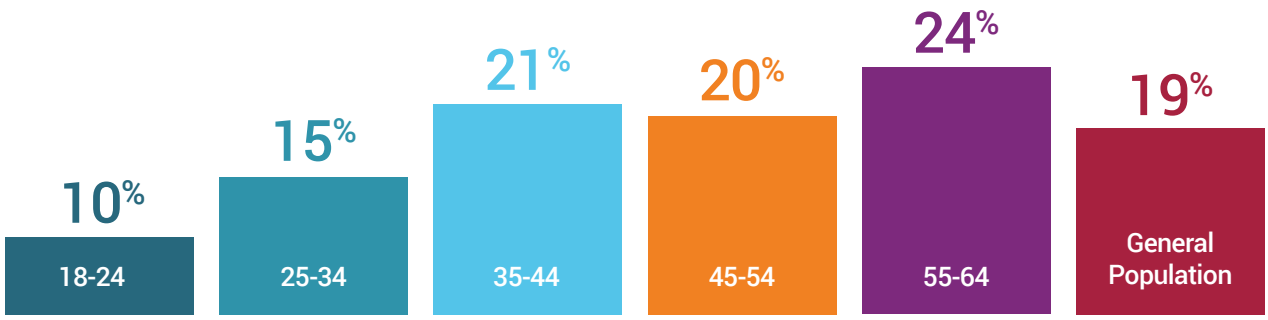


Note: These percentages reflect the percentage of respondents who reported they were a 4 (very concerned) or a 5 (extremely concerned) across each of the above ways companies interact with their data.

Source: Consumer Perceptions of Privacy in the Internet of Things, Altimeter Group, 2015 Base: n=2062 respondents

FIGURE 6C COMPARISON OF EXTREME CONCERN ACROSS AGE GROUPS

Percentage of respondents who rated themselves "extremely concerned" (5/5) across all categories of data use



Note: This chart shows variation of extreme concerns across age groups (those who rated a 5/5 where 5 is extremely concerned)

Source: Consumer Perceptions of Privacy in the Internet of Things, Altimeter Group, 2015 Base: n=2062 respondents

This is significant given the pervasive sentiment that millennials and younger populations could 'care less' about privacy. While these segments may be more prone than their elders to sharing information about themselves digitally, concerns around privacy are not solely a function of age. Areas of concern and parameters for what constitutes 'personal' or 'sensitive' may be different, but age is far from the only factor accounting for variations in such sensitivities. Privacy, or the desire of an individual or group to seclude themselves, information about themselves, and thereby express themselves selectively, is innately human."[12]

CONSUMER CONCERNS SIGNAL DEEP LACK OF CONSENT, AWARENESS, AND COMFORT

Altimeter data suggest great concern when it comes to when, where, how, and with whom companies use or share consumer data. The data also show a desire for awareness, transparency, consent, and control. A recent survey by TRUSTe found that 85% of consumers wanted to understand more about how their data is collected before using connected devices. Just 20% of respondents feel that the benefits of smart devices outweigh their privacy concerns; 80% disagree.[13]

In Altimeter's survey, (a quantitative survey of general consumers sourced and vetted through a panel provider,) the outpouring of qualitative feedback we received in a box merely titled 'Comments' reinforces this:

What businesses must understand is that this data doesn't just suggest a concerned citizenry, it suggests a fundamental barrier to realizing the potential (and capitalizing on their investments) in the Internet of Things. It represents a call for intervenability, an imperative to place control, consent, and agency back into the hands of those providing the data for whom IoT is intended to benefit: consumers.

III. COMPANIES MUST RESPOND TO CONSUMER CRIES FOR VALUE CREATION, CONTROL, AND TRANSPARENCY

There are numerous questions businesses should ask in light of these explicit concerns, both immediately and over time as IoT matures. Today and increasingly, companies are facing a very real 'trust imperative'[14] — an existential imperative to foster trust with consumers, for risk of failure, security compromise, customer safety, and ethical responsibility. This calls for a transformation, not only in the way businesses collect, process, analyze, store, secure, govern, and use consumer data, but in the design of the experience as well as how they communicate directly with consumers about this use. Because it's not just risk mitigation and existential threat; it's pragmatic; it's an exchange; it's just good business.

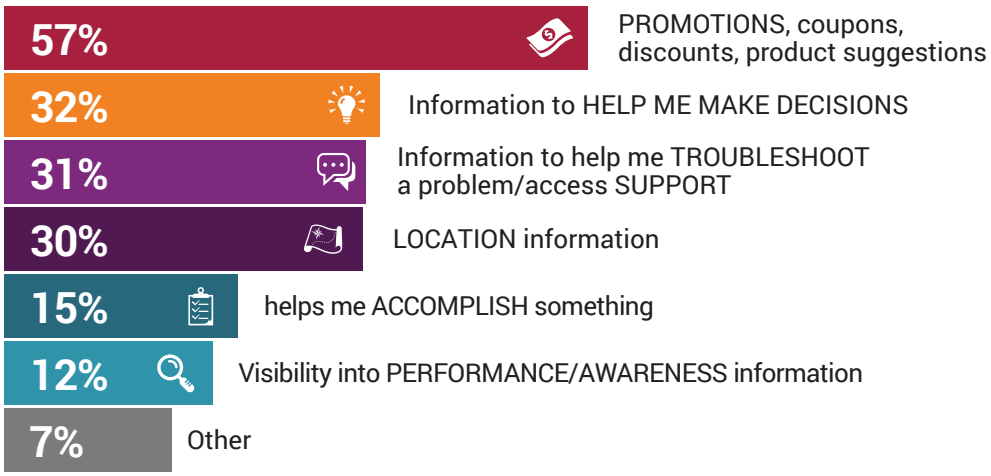
DESIGNING FOR VALUE EXCHANGE ISN'T JUST ABOUT UTILITY, IT'S ABOUT TRUST

A second, perhaps more immediate question applicable to every consumer-facing function and program is what constitutes a valuable experience? This question is more important that it has ever been for two reasons:

- **Just because we can now add sensors to [any] thing… doesn't necessarily mean we should.** Yet we're seeing companies race to connect their products, in-store environments, and build mobile apps. This year's Consumer Electronics Show brought us connected flowerpots, Bluetooth enabled tape measures, (smart?) rubber duckies, among others.[15] But adding a sensor to something does not magically endow it with value for its user, particularly when weighed against potential risks. One study found that the top reason consumers hadn't purchased in-home connected devices was because they didn't understand the value.[16] Gone are the days when simply connecting something to the Internet sufficed as a differentiator.
- **A valuable brand experience fosters trust.**
  As distrust has quantifiable impact on business performance[17], so too does trust. The 2015 Edelman Trust Barometer, a survey of over 33,000 consumers, found that 80% chose to buy products and services from companies they trusted; they also were more likely to recommend them to a friend, pay more for them, and even purchase shares in the company.[18] Value breeds trust and loyalty, and in turn, trust and loyalty breed value for the company.

FIGURE 7 CONSUMERS MOST COMPELLED TO SHARE THEIR DATA IN EXCHANGE FOR SAVINGS—MONEY, TIME, AND ENERGY

Q: Which of the following reasons do you find most compelling or valuable to share your data with companies? (Select your top 3)



Source: Consumer Perceptions of Privacy in the Internet of Things, Altimeter Group, 2015 Base: n=2062 respondent

Companies must begin to address the question of value exchange by empathizing with consumers around the *'why?'* and *"what's in it for me to share my data with a business?"*

In a world where the use of data can both serve and sour consumers, businesses must be asking this question at every turn. Altimeter's survey finds, perhaps to no surprise, that when it comes to compelling reasons to share data, monetary incentives top the list. (See figure 7) 57% of respondents cite promotions as the most compelling reason to share their data.

Another theme emerges from this data—savings. Whether in the form of money, time, or energy, consumers are most incentivized to share their data by gains in efficiency. Indeed not all 'value exchange' is created equal; this study finds that consumers with higher trust place higher value on information to aid with decision-making, where as those with lower trust are more compelled to share their data for customer support needs. These particular findings address a deeper question: are coupons really enough?

A recent study by the University of Pennsylvania's Annenberg School of Journalism finds that willingness to share is less a function of affinity for discounts, and more a function of what the authors term, "resignation."[19] The report defines resignation as what happens "when a person believes an undesirable outcome is inevitable and feels powerless to stop it." The study asked consumers if they felt discounts were indeed a fair exchange for marketers to collecting information about them without their knowledge; 91% of respondents disagreed. Rather, the study claims, most Americans disclose their personal data to companies for discounts because they believe that marketers will harvest the data anyway.

It's no secret the Internet of Things market is growing rapidly. Investment in sensors and connectivity by industry and governments around the world is soaring to the tune of billions of dollars.[20] Yet amidst this frenzy of activity, there is an obscured truth: when companies think about the opportunity of consumer device data, they think foremost in terms of innovation and monetization, and less about privacy protection or communications and disclosure. Businesses must bridge the gap between innovative potential and consumer awareness.

CONTROL, AWARENESS, AND THE GREAT GAP BETWEEN UNDERSTANDING AND INFORMED CONSENT

There is a schism between the momentum we see by those developing connected products, infrastructure, and services, and the everyday consumers who are expected to adopt it. A wider understanding of the ways businesses can, and to a great extent, already are, using customer data is limited today. A recent study by Harvard Business Review found only about a quarter of consumers even realize they are sharing their data when they go online.[21] The study by University of Pennsylvania reveals a host of consumer misconceptions about how consumer data is [not] protected from discriminatory pricing schema.[22]

- **69%** do not know that a pharmacy does not legally need a person's permission to sell information about the over-the-counter drugs that person buys.
- **65%** do not know that the statement "When a website has a privacy policy, it means the site will not share my information with other websites and companies without my permission" is false.

Consumers may be resigned to not resisting the typical registration or exchange process of [all of your] data for the service, but they are not disinterested. They may be naïve about what protections exist (or don't), but they aren't stupid. The industry has set a precedent for terms of service and privacy agreements that are difficult to access, read, and understand, but this level of obscurity will no longer suffice. It is in companies' best interest to educate consumers, to differentiate themselves through visibility and value exchange; not remain complicit in user ignorance, or worse, unaccountable for the destinations of such data once it has left their servers or clouds.[23] If companies want to realize their investments, and more importantly, the potential of IoT, they must take steps to bridge the very gap they helped create in the first place. As inputs for consumer data permeate the physical world, a structure based on trust and transparency is in order.

RESEARCH REVEALS OPPORTUNITIES FOR BRANDS TO ENGAGE MORE STRATEGICALLY AND ETHICALLY

This study reveals consumers have significant interest in learning more about privacy protections and receiving notifications across more environments, even more platforms. Amid the confusion, distrust, and interest in learning more lies an opportunity for brands to communicate, educate, and engage more effectively.

We are still in the very early days of the Internet of Things. Brands can see this as a signal to 'wait and see,' to follow the status quo of obscuring information from already distrusting consumers. Or they can see what a massive differentiator it is to forge trust and loyalty, communicate clearly and ethically, and equip themselves with better legal templates and protections. After all, the more companies have considered, planned for, documented, communicated, and accounted for in the way of data privacy and security strategy, the better they will fare in court should such an event come to pass. Following are a few simple ways companies can begin.

1. USE EDUCATIONAL MATERIALS, TOOLS, OR OTHER RESOURCES TO DIFFERENTIATE

The opportunity for brands to serve as facilitators, partners, and educators of the risks (and opportunities!) around consumer data is tremendous. We are in a unique moment in technological innovation when, through sensors and connectivity, companies can help empower consumers to do— to control, to see, to react, to fix, to accomplish.[24] Providing agency and intervenability around consumer data is a natural extension of this.

The Digital Advertising Alliance (DAA) recently released 'App Choices,' a mobile app offering consumers simplified means to control data collection and use across individually-named DAA companies, or all participating companies at once.[25] Data broker Acxiom hosts an online portal called www.aboutthedata.com for self-service education, visibility, and the ability to edit or opt-out of their marketing products.[26] Could companies offer heightened protection services, contests, even create new revenue models? Is there an opportunity in brands helping consumers monetize their own data? The model of clandestine data use and abuse is ripe for disruption.

- ☑ Provide informational resources (e.g. disclosures, partner lists, risks, opportunities, 3rd party resources or tools, risk assessment tools)
- ☑ Provide portals for action (e.g. mobile apps, web portals, dashboards, 3rd party tools or templates, support, incentives)

2. ALLOW FOR OPT-IN, OPT-OUT, OPTIONS AT THE GRADIENT LEVEL

Today the standard for communicating to consumers about how their data is used, stored, and shared is the Terms of Service (TOS) agreement. Many businesses today communicate these agreements using complex statutes and legalese, circumventing the need to communicate in clear and efficient ways with consumers. Sometimes the consumer registration process merely includes a link to the ToS and privacy policy, with "agree" selected by default. From a business perspective, the role and design of these user agreements is not to protect consumers by educating them and soliciting informed consent, it is primarily to protect businesses from legal sanction.

The current precedent has conditioned end users to literally 'accept' a long, complicated series of paragraphs typically written in legalese in order to enjoy a service or sign up for a product. Businesses shouldn't necessarily

assume users are comfortable with a default of opt-in to all features or sensor settings. If a user is uncomfortable enough to refuse, they can't use the service at all. The gates of a one and done, binary Yes/No, all-in/all-out agreement are the norm. Our research found that consumers most prefer periodic updates, sent over email and able to be tracked over time, followed in preference by event-triggered notifications, not the one-time model of Terms of Service. To this point, it is worth mentioning the inherent value in cleansing a customer base of disinterested, even disgruntled users, which only adds to the purity, longevity, and effectiveness of such a list of contacts. Indeed, for skeptical or 'resigned' prospects, gradient controls could help foster trust and increase the chance of greater investment later—in the form of dollars, data, or loyalty. Businesses have an opportunity to change this model: to allow for a 'dial' or menu of privacy controls, instead of an on-off switch.

- [x] Provide users options in the collection, use, sharing, storage of their data
- [x] Provide users options in the frequency in which they can update these options
- [x] Provide users options in the channels in which they can update these options

3. UNDERSTAND TECHNOLOGICAL EXPOSURE AND ENGAGE ACCORDINGLY

When it comes to concerns and interest around privacy, the research signals a clear distinction between those with greater exposure to technology vs. those less exposed. Those with greater exposure welcome more outreach and signal greater interest in learning more. 'Exposure' to technology can manifest in various ways, such as the number of devices owned, how much they know about specific types of technologies, age, life stage, or if they live in a densely or sparsely populated environment. Companies should place greater emphasis on engaging these groups with informational and educational materials, but also take advantage of their technological savvy.

- [x] Provide new channels and/or frequency of notification and monitor their response
- [x] Test new campaigns for building awareness and transparency
- [x] Provide them more control over the use and sharing of their data and monitor these interactions
- [x] Ask them for feedback and adjust

4. CRAFT ENGAGEMENT TO REFLECT (AND RESPECT) DEPTH OF EXISTING RELATIONSHIP

Understand where you are in your relationship with customers when considering how to message them around privacy terms and risks. This may seem obvious, but the standard operating procedure when it comes to privacy notification (of running every user through a single gate, the Terms of Service) doesn't reflect this approach. While some privacy notifications will be standardized, the greater point is that not all consumers will have the same level of awareness, openness, affinity, trust, or loyalty to you as a brand. This is particularly important for companies taking on new IoT initiatives, as these activations assume significantly more risk (to both brand and consumer) around privacy, data [mis]use, security, safety, and of course, wasted investment. Companies must balance this risk by providing clear notifications tailored to the level or depth of the existing relationship.

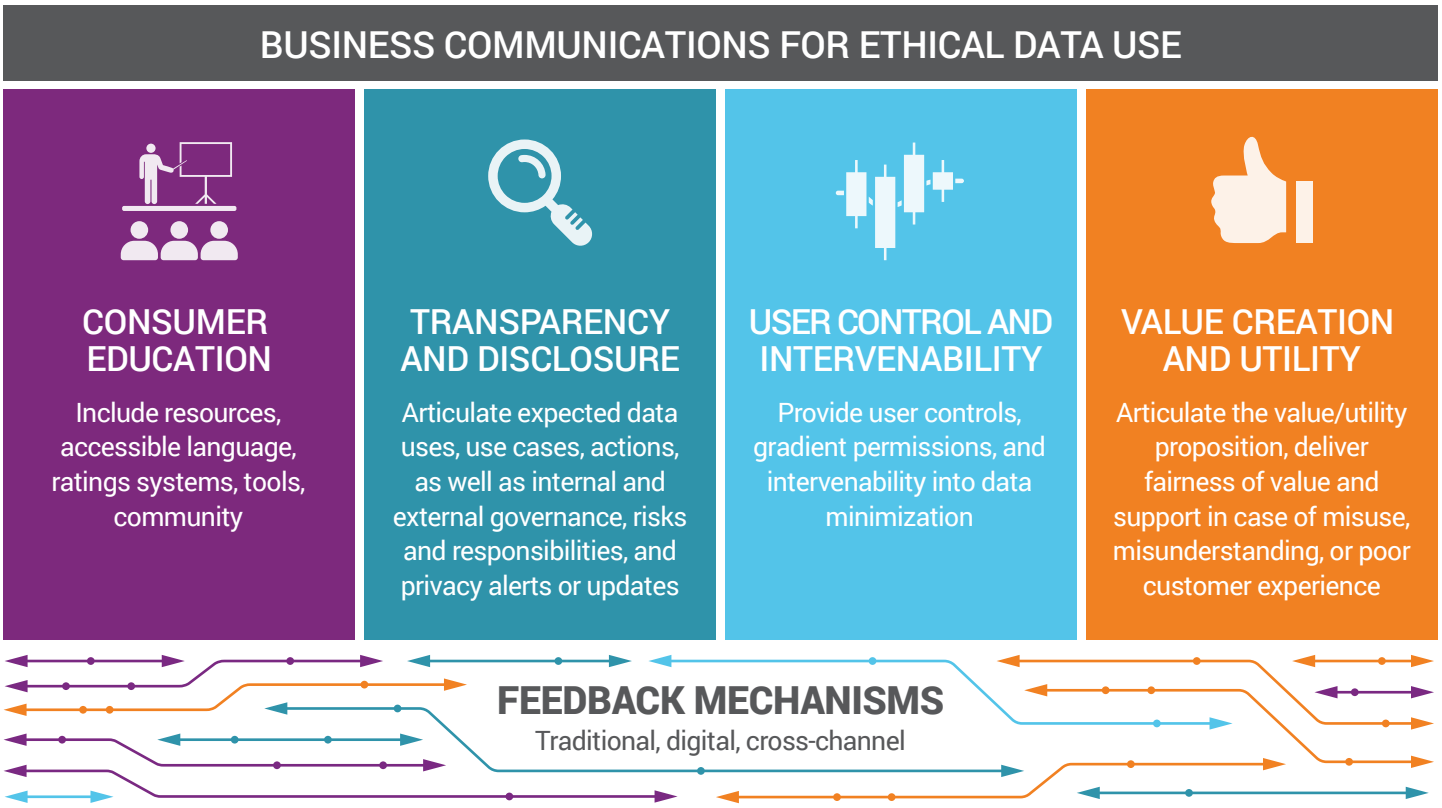
- [x] Develop clear triage for how experience differs based on depth of existing relationship; provide options to customize these settings
- [x] Tailor messaging and call-to-action (CTA) to depth of existing relationship (prospect, customer, loyalty member, advocate, etc.)
- [x] Incentivize deeper engagement through incremental outreach, reflecting depth of relationship (e.g. persona or engagement history)

5. ADHERE TO THE FUNDAMENTALS OF ETHICAL DATA USE AND COMMUNICATION

The central imperative and responsibility brands have when leveraging consumer data is to manage it ethically. Altimeter Group's research report, "The Trust Imperative," lays out a framework for ethical data use.[27] This framework is based on principles developed by the Information Accountability Foundation (IAF) that define ethical data use as: beneficial, progressive, sustainable, respectful, and fair.

Companies must apply these principles, not just to the use—the collection, processing, analysis, governance, storage and security—of the data, but to communications about these elements as well. The subject of upcoming Altimeter research is precisely this; a framework specifically for ethical, accessible, and transparent communications of the use of consumer data. Just because consumers may not always read through the Terms of Service or Privacy Policies doesn't mean they lack a desire to understand, access, and control more. Companies can begin bridging the gap of understanding and trust by aligning their messaging and experiences against the following four pillars of ethical data communications: (See figure 8)

FIGURE 8 FOUR PILLARS FOR BUSINESS COMMUNICATION ABOUT CONSUMER DATA



CONCLUSION

There is an inherent friction to privacy. Companies may point to a cumbersome user experience, legal complexity, or other reason for 'streamlining' registration processes, communications about privacy, or minimizing notifications of data use. But, perhaps there should be friction in privacy. Privacy is not something we can standardize or account for in a scripted template. It is a function of shifting contexts, motives, and frameworks: culture, religion, location, age, gender, income, family, sexual orientation, life events, experiences, exposure, and more. Privacy is subject to each of our unique, yet deeply human sensitivities. It is as ingrained in us, indeed related to, our innate imperative to maintain status in order to more effectively propagate forward our genes.

"The tectonic shifts we're seeing in technology are not matched by such dramatic shifts in human behavior. Culture, values, norms, politics, how we interrelate with one another– these things change slowly."

--Gilad Rosner, Founder of IoT Privacy Forum

As a species we have had roughly 100,000 years to develop our behavioral norms in the physical world; but we have had barely 100 years to develop such norms in the digital world. As a society, we all face the potential to both suffer and benefit from a connected world. It is the responsibility of the entities that are digitalizing our physical world to educate, to safeguard, and to help foster new, responsible behavioral precedents in the Internet of Things.

ENDNOTES

[1] This survey represents a general distribution of American consumers, based on US census data for demographic distributions sourced in 2010. Altimeter sourced these respondents through a panel provider which used a three-part opt-in for consent. This data is based on a panel sample that was conducted and monitored to mirror this distribution.

[2] "The Internet of Things: Can It Find a Foothold With American Audiences Today?" Nielsen, November, 2014. http://www.affinnova.com/resource-story/internet-of-things/.

[3] 2015 US Consumer Confidence Privacy Index, TrustE https://www.truste.com/about-truste/press-room/americans-online-privacy-more-important/.

[4] 2014 US Consumer Data Privacy Study: Consumer Privacy Edition, TRUSTe http://www.slideshare.net/trusteprivacyseals/2014-us-consumer-data-privacy-study-consumer-privacy-edition-from-truste.

[5] Timothy Morey, Theodore Forbath and Allison Schoop, "Customer Data: Designing for Transparency & Trust," Harvard Business Review, May 2014 https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust.

[6] Although not included in this report, the data from this survey will help inform a framework for ethical communications businesses can adopt to better engage, build trust, and educate consumers around the use of their connected device data.

[7] "The Internet of Things and the Future of Consumer Adoption," Acquity Group, 2014. http://www.acquitygroup.com/docs/default-source/Whitepapers/acquitygroup-2014iotstudyfca32e3440236f7b9704ff000083d49c.pdf?sfvrsn=2.

[8] This survey represents a general distribution of American consumers, based on US census data for demographic distributions sourced in 2010. Altimeter sourced these respondents through a panel provider which used a three-part opt-in for consent. This data is based on a panel sample that was conducted and monitored to mirror this distribution.

[9] "comScore reports January 2015 U.S. Smartphone Subscriber Market Share," comScore http://www.comscore.com/Insights/Market-Rankings/comScore-Reports-January-2015-US-Smartphone-Subscriber-Market-Share.

[10] Gil Press, "Internet of Things by the Numbers," Forbes, 22 Aug 2014 http://www.forbes.com/sites/gilpress/2014/08/22/internet-of-things-by-the-numbers-market-estimates-and-forecasts/.

[11] Mary Madden and Lee Rainie, "American's Attitudes About Privacy, Security, & Surveillance," Pew Research Center, 20 May 2015 http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

[12] Wikipedia contributors, "Privacy"Definition of privacy, Wikipedia, The Free Encyclopedia, date accessed June 24, 2015 http://en.wikipedia.org/wiki/Privacy.

[13] 2014 TRUSTe Privacy Index: Internet of Things Edition, TRUSTe, February 2014 https://www.truste.com/resources/privacy-research/us-internet-of-things-index-2014/.

[14] Susan Etlinger, "The Trust Imperative: A Framework for Ethical Data Use," Altimeter Group, June 2015, http://pages.altimetergroup.com/The-Trust-Imperative-Report.html.

[15] Jessica Groopman, "Welcome to the Internet of …Yawn, More Things," Altimeter Group Blog, January 2015 http://www.altimetergroup.com/2015/01/ces-2015-the-internet-of-yawn-more-things/

[16] "The Internet of Things and the Future of Consumer Adoption," Acquity Group, 2014. http://www.acquitygroup.com/docs/default-source/Whitepapers/acquitygroup-2014iotstudyfca32e3440236f7b9704ff000083d49c.pdf?sfvrsn=2.

[17] Susan Etlinger, "The Trust Imperative: A Framework for Ethical Data Use," Altimeter Group, June 2015, http://pages.altimetergroup.com/The-Trust-Imperative-Report.html.

[18] "2015 Edelman Trust Barometer," Edelman, 2015 http://www.edelman.com/2015-edelman-trust-barometer-2/trust-and-innovation-edelman-trust-barometer/executive-summary/.

[19] Joseph Turow, Ph.D., Michael Hennessy, Ph.D., Nora Draper, Ph.D., "The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening them Up to Exploitation," University of Pennsylvania Annenberg School of Communications, June 5, 2015 https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

[20] Joao Lima, "Behold the 10 biggest IoT Investments" Computer Business Review, April 9 2015 http://www.cbronline.com/news/internet-of-things/behold-the-10-biggest-iot-investments-4549522.

[21] Morey, Forbath and Schoop, "Customer Data: Designing for Transparency & Trust," Harvard Business Review, May 2014 https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust.

[22] Turow, Hennessy, Draper, "The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening them Up to Exploitation," University of Pennsylvania Annenberg School of Communications https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

[23] Michael Fertik, "Big Data, Privacy, and the Huge Opportunity in the Monetization of Trust," The Nation, January 25, 2012 http://www.nationmultimedia.com/technology/Big-Data-Privacy-and-%20the-Huge-Opportunity-in-the-M-30174527.html.

[24] Jessica Groopman, "Customer Experience in the Internet of Things: Five Ways Brands can Use Sensors to Enhance Customer Relationships," Altimeter Group, March 2015 http://www.altimetergroup.com/2015/03/new-research-customer-experience-in-the-internet-of-things/.

[25] Michael Barris, "DAA App, Web Page ease control of mobile ad views," Mobile Marketer, February 25, 2015 http://www.mobilemarketer.com/cms/news/advertising/19848.html.

[26] "Aboutthedata.com," Axciom, 2015 https://aboutthedata.com/portal/registration/step1, Date Accessed June 24, 2015.

[27] Susan Etlinger, "The Trust Imperative: A Framework for Ethical Data Use," Altimeter Group, June 2015, http://pages.altimetergroup.com/The-Trust-Imperative-Report.html.

METHODOLOGY

This study surveyed a sample of 2062 American consumers sourced through an online survey panel. In order to achieve a general distribution of American consumers, as defined by age, living environment, region, and gender, respondents were triple vetted by the panel provider and modeled against the 2010 U.S. Census Bureau data. The survey was conducted during the month of May 2015.

ACKNOWLEDGEMENTS

I would like to convey my gratitude to all of the brilliant and influential individuals and institutions I have found throughout my research of IoT and privacy. While additional artifacts containing their input are coming soon, I extend special thanks to Dr. Gilad Rosner, Jared Bielby, Lee McKnight, Geoff Webb, Oleg Logvinov, the IEEE, Robert Nievert, Sean Lorenz, Paddy Srinivasan, Elliot Katz, Chris Massot, Todd Rytting, Mark Wright, and Craig Speizel, and the Online Trust Alliance.

Additional thanks due to insights and/or support from Rebecca Lieb, Charlene Li, Shannon Latta, Vladimir Mirkovic, Ed Terpening, Omar Akhtar, Briana Schweizer, and Solène Lejosne. Finally, a special thank you to my whip smart colleague, friend, and mentor in research on ethical data use and communications, Susan Etlinger.

OPEN RESEARCH

This independent research report was 100% funded by Altimeter Group. This report is published under the principle of Open Research and is intended to advance the industry at no cost. This report is intended for you to read, utilize, and share with others; if you do so, please provide attribution to Altimeter Group.

PERMISSIONS

DISCLAIMER

About Us

Jessica Groopman, Industry Analyst

Jessica (@jessgroopman)is an industry analyst with Altimeter Group, where she covers the Internet of Things. The focus on her research is on the application of sensors for consumer-facing businesses, with an emphasis on customer experience, privacy, contextual marketing, automated service, and wearables. She is featured on Onalytica's top 100 influencers in the Internet of Things. Jessica blogs about her research at jessgroopman.com and is a regular contributor to numerous 3rd party industry blogs. She is also a contributing member of the FC Business Intelligence IoT Nexus Advisory Board and the International IoT Council. Jessica has experience conducting business, technological, and anthropological research.

Susan Etlinger, Industry Analyst

Susan Etlinger (@setlinger) is an industry analyst at Altimeter Group, where she works with global organizations to develop data and analytics strategies that support their business objectives. Susan has a diverse background in marketing and strategic planning within both corporations and agencies. She's a frequent speaker on social data and analytics and has been extensively quoted in outlets, including *Fast Company, BBC, The New York Times,* and *The Wall Street Journal*. Find her on LinkedIn and at her blog, Thought Experiments, at susanetlinger.com.

About Altimeter Group

Altimeter is a research and consulting firm that helps companies understand and act on technology disruption. We give business leaders the insight and confidence to help their companies thrive in the face of disruption. In addition to publishing research, Altimeter Group analysts speak and provide strategy consulting on trends in leadership, digital transformation, social business, data disruption and content marketing strategy.

How to Work with Us

Altimeter Group research is applied and brought to life in our client engagements. We help organizations understand and take advantage of digital disruption. There are several ways Altimeter can help you with your business initiatives:

Strategy Consulting. Altimeter creates strategies and plans to help companies act on business and technology trends, including ethical and strategic data use and communications. Our team of analysts and consultants work with global organizations on needs assessments, strategy roadmaps, and pragmatic recommendations to address a range of strategic challenges and opportunities.

Education and Workshops. Engage an Altimeter speaker to help make the business case to executives or arm practitioners with new knowledge and skills.

Advisory. Retain Altimeter for ongoing research-based advisory: conduct an ad-hoc session to address an immediate challenge; or gain deeper access to research and strategy counsel.

To learn more about Altimeter's offerings, contact sales@altimetergroup.com.