WHERE WE ARE IS WHO WE ARE

THE HIGH STAKES OF GETTING LOCATION DATA RIGHT
In an online world, every piece of data we generate is a part of who we are. It describes us, our age and gender, our habits and preferences, where we work and live, who we know and who we know well. Location data, more than any other, tells our unique story. Every meaningful interaction, every night’s sleep, every vacation, every purchase, every journey, every waking hour happens at a specific place. Where we are is who we are.

Knowing what consumers like and dislike is hugely valuable to any technology marketer, of course. Knowing where consumers are and what they’re doing at any point in time takes that value to another level. But, perhaps understandably, it’s information that consumers are only happy to provide in exchange for real benefits. And they won’t want to provide it at all unless they trust the organization that they are dealing with.
Accenture’s 2019 Digital Consumer Survey¹ found that more than half (58%) of all online consumers believe that sharing their location data poses personal risk. So how can companies respect users’ privacy while providing location-aware services?

Some of the most valuable smartphone-enabled experiences rely on a user’s location data. From maps and navigation to weather forecasts and from local search to ride-sharing, knowing a consumer’s precise location is essential to provide the most relevant and timely experience. With the rise of wearable technology, connected vehicles and smart urban environments there’s more potential value from geo-location than ever.

Recent research from Accenture has also identified new experiences “at the edge”—at the intersection of the physical and digital world, like delivery into the home and driverless taxis—which will further shape attitudes and behaviors.² At a time when only the most relevant will survive, the potential for companies to be present “in the moment” with their customers is an unmissable opportunity.
WHY IS LOCATION DATA SO VALUABLE?

Knowing where someone is and what they are doing creates a huge range of commercial opportunities for companies. Fertile consumer scenarios range from highly targeted advertising to geo-fencing and from logistics to home automation. There’s value in other areas too, from field worker safety to emergency services dispatch.

According to eMarketer, US mobile location-targeted ad spending will more than double between 2017 and 2022, from $17.1 billion to $38.7 billion; 58% of retailers plan to invest in location-based marketing. The ride-sharing industry’s growth is predicated on users sharing their location data, with estimates suggesting that these companies already provide 15 million rides globally each day, expected to hit 97 million by 2030 (when the annual market for these services could be worth $285 billion). That’s not all. Some billion-dollar valued businesses, like Waze and Nextdoor, have been specifically created from users’ desire to share and gain from sharing their location and local data with millions of others.

58% of retailers plan to invest in location-based marketing.
WHERE CONSUMERS STAND ON LOCATION

That’s the good news. The bad news? Location data can be misused, representing a real threat to personal security and property. Companies that fail to adequately protect their customers’ location data could take a serious financial and reputational hit.

Most consumers do continue to share their location. In fact, we found that 82% of all consumers use apps that require location data (no surprise that those aged 35 and under are the most likely to do so, with 89% of 14-24-year-olds relying on apps that use their location). But what consumers share, when and with whom varies according to where they live, their age and their gender. Only a minority of consumers, just 15% of all global consumers, are comfortable sharing their location data all the time. However, an even smaller minority, 6%, is never willing to share.

Fig 1: Situations in which consumers share Smartphone location data.

<table>
<thead>
<tr>
<th>Situation</th>
<th>% of Consumers</th>
</tr>
</thead>
<tbody>
<tr>
<td>63% directions</td>
<td></td>
</tr>
<tr>
<td>48% check weather</td>
<td></td>
</tr>
<tr>
<td>34% local recommendations</td>
<td></td>
</tr>
<tr>
<td>29% get a taxi</td>
<td></td>
</tr>
<tr>
<td>27% social media</td>
<td></td>
</tr>
<tr>
<td>20% ride sharing</td>
<td></td>
</tr>
<tr>
<td>17% news</td>
<td></td>
</tr>
<tr>
<td>13% sports</td>
<td></td>
</tr>
<tr>
<td>12% video</td>
<td></td>
</tr>
<tr>
<td>12% gaming</td>
<td></td>
</tr>
<tr>
<td>10% dating</td>
<td></td>
</tr>
</tbody>
</table>

In which situations do you share access to your smartphone location data?
The willingness to share personal location data is in large part a result of the value that location-aware apps are seen to deliver. Most consumers (63%) are willing to share their location for directions, with checking the local weather the next most common choice at 48% of all consumers. Information and search about local services, such as restaurant recommendations and hailing a taxi come next with 34% and 29%, respectively. For other common digital activities, such as dating, gaming and accessing content, only around 10% of consumers are happy to share their whereabouts.

It’s generally the younger, more urban consumers that are most inclined to share location data. But they are also most wary about the potential for unauthorized data use that sharing their location may expose them to: 62% of 18-24-year-olds express concern about this, compared with 55% of those aged over 65. Gender plays an influential role, too. We found that women are more likely to be cautious about sharing their location than men, especially when it could reveal exactly where they are at a given moment in time. There are also marked differences between countries. Consumers in Brazil, China, India and Mexico are more likely to share location than those in more privacy-concerned countries like France, Germany and the Netherlands.

Gender plays an influential role, too. We found that women are more likely to be cautious about sharing their location than men, especially when it could reveal exactly where they are at a given moment in time.
Nearly everyone used to be happy to provide another form of location data: their address. It has always been possible for companies and others to contact us at home via direct mail or telephone if our details were listed. So what’s changed? The difference today is that with the possibility of real-time and constant measurement of presence, the individual is not simply associated with a static address and/or phone number. Today, our location data provides a constant stream of accurate data about us.

That’s why we’re seeing so much emphasis today on using this unprecedented power responsibly. Two US mobile operators recently announced that they would no longer sell location data to third parties, while a weather app provider was sued, accused of sharing location data with advertisers and affiliates of its parent company. And with the adoption of GDPR in Europe, the use of location data has come under ever-closer security, with fines already imposed for breach of the EU’s data protection rules.
Leading companies are harnessing public and regulatory concern about location data and privacy by promising not to exploit or sell it in their services. In Apple’s announcement of its new mapping data program, it described in some detail how it used location data, disaggregating GPS traces into anonymized segments to ensure personally identifiable information such as journey to work could not be inferred. Trust in location data can be a persuasive brand value.

The stakes are becoming higher due to the near-ubiquity of the smartphone (millions of us carrying an always-on, internet-connected device, associated with us uniquely), the cloud (bringing the sensor data from the IoT into one place) and big data (the ability to make sense of all that data). With location sensors and applications that require ongoing access to the individual’s location to function, the result is a constant stream of location data associated with a specific individual. If that data is retained and processed with advanced, predictive analytics it can be used to target or proactively intervene in consumers’ lives based on their past activity and movement.

While all of this creates real value for consumers, that gain is offset by some significant new threats. If location data gets into the wrong hands, consumers’ personal security can be put at risk. With that information, criminals would be able to know exactly where someone would be and at what time.

Home security can be compromised, with would-be intruders knowing when a property is vacant. Personal privacy can be violated if meeting locations are known. Overall, the implications of breaches in the confidentiality of location data run from the merely annoying, such as unwanted ads and offers, to the creepy, to the dangerous in scenarios where personal safety is directly threatened.
If the relationship between the consumer and company around location data is strong, a very powerful business can be built on top. The rise of companies like Uber, Lyft, Didi and Grab underline the very obvious value exchange that trust empowers. However, consumer expectations of who should be responsible for keeping their location data safe vary considerably. For example, in the US, UK, Germany, Japan and Australia, it’s the device OS provider. In India and China, it’s the smartphone provider, and in France and Mexico, it’s the telco.

Fig 2: Trust is a differentiator, negative or positive, and location cuts across key risk factors.

To reap the benefits of location data and guard against the potential risks it creates, companies must develop the right policies and culture based on a very clear understanding of specific markets and geographies. These will, above all, need to inspire consumer trust. As trust becomes an indispensable brand attribute for technology companies, heightened scrutiny on how they handle permission and use of location data is fundamental.
We see four key questions that every technology company must be able to answer if they want to earn and protect trust in their handling of location data:

01 **TRANSPARENCY**
do users know how a company is using their data?

02 **CONTROL AND CONSENT**
can users fully control what data they share and what consent they provide?

03 **EXPERIENCE**
are users confident they will have the safe and secure experience they expect in the value exchange?

04 **CERTAINTY**
can users be certain that their data is only being used in their best interests and to achieve the outcomes they’ve envisaged?

Companies can respond to these questions by making the location/value trade-off explicit to each consumer, including any resale of location data to partners. Easy-to-use “right to be forgotten” requests and controls visibility into where location data has been provided should feature on each consumer’s profile page.

Offering tiers of location awareness to consumers, with the option for them to allow granularity by, say, street, borough or state, would provide reassurance. So would allowing the device itself to sort the location data.

For example, if the company knows a consumer is in San Francisco or one of its neighborhoods, it could send ads for selected restaurants and movie theaters to their device and allow the device itself to decide if they’re near one of them. If that’s the case, the device offers the ad and reports that back anonymously. The ad is delivered to the customer, and their personal location is not compromised.
Today’s platform companies recognize that geospatial is critical to disruptive innovation. They’re making big bets to build capabilities in shared mobility, autonomous vehicles, last-mile delivery, augmented reality and virtual reality, IoT and geospatial analytics.

As organizations size up and attack the massive geospatial opportunity, it is imperative to marry strong strategy with strong execution, agility and innovation – with a critical eye to quality, customer experience and trust.

There are three concrete steps companies should take now to address the important issues of trust inherent in location data:

01 Establish Data Ethics Leadership
Develop a focal point within the company for addressing data ethics challenges across products and services. Companies should establish the principles of their data ethics program and begin socializing these principles with the key leaders (including CTO, CIO and General Counsel) who can empower internal data ethics leadership to shape the agenda and effect change. They should also include an external statement about location data and how it will be used in their customer-facing messaging. Make the trade-off explicit. Provided the value proposition is attractive, users will be likely to agree with it.

02 Design and Build for Trust
Deploy robust DevSecOps and Privacy by Design capabilities and tools to empower every engineer and product team with the resources to build trusted products and services at the beginning of the development lifecycle, with the know-how necessary to address the specific challenges of location data.

03 Partner Internally to Enable Innovation
Trust teams should be part of the strategic planning process, working to proactively identify opportunities to accelerate the innovation agenda. Traditional trust functions must shift from being compliance workloads to product development and engineering workloads.
About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 477,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

To find out more about how Accenture’s Geospatial Platforms and Trust and Security teams are helping clients with these and related challenges, please contact:

Matthew Quinlan
Principal Director, Geospatial Platforms
Accenture Software & Platforms
matthew.h.quinlan@accenture.com

David M. Cooper
Global Privacy Lead
Accenture Security
david.m.cooper@accenture.com

Paul Johnson
Senior Principal, Global Research
Accenture Software & Platforms
paul.d.johnson@accenture.com

References

1 Accenture’s 2019 Digital Consumer Survey explored the question of location data, asking consumers in 21 countries around the globe how they share location data, why, how they feel about it and who they trust with it.


Copyright © 2019 Accenture. All rights reserved.

Accenture and its logo are trademarks of Accenture.