SURVEY ANALYSIS REPORT

CONNECTED LIVING:
THE VOICE OF THE CONSUMER

WHAT DO THEY EXPECT THEIR IoT EXPERIENCE TO BE IN 2030?
<table>
<thead>
<tr>
<th>Section</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2-3</td>
</tr>
<tr>
<td>Scope of research/methodology</td>
<td>3</td>
</tr>
<tr>
<td>The ideal IoT experience in 2030: a day in the life</td>
<td>4-5</td>
</tr>
<tr>
<td>Summary of key findings</td>
<td>6-7</td>
</tr>
<tr>
<td>1. How will IoT impact lives in 2030?</td>
<td>8</td>
</tr>
<tr>
<td>2. The future of IoT and consumer experience</td>
<td>9-14</td>
</tr>
<tr>
<td>IoT devices and smart services</td>
<td>11</td>
</tr>
<tr>
<td>Artificial Intelligence (AI)</td>
<td>12-13</td>
</tr>
<tr>
<td>Silent authentication</td>
<td>14</td>
</tr>
<tr>
<td>3. Security of IoT devices</td>
<td>15-18</td>
</tr>
<tr>
<td>Conclusion</td>
<td>19</td>
</tr>
<tr>
<td>About Gemalto</td>
<td>20</td>
</tr>
<tr>
<td>Contributors</td>
<td>21</td>
</tr>
</tbody>
</table>
Despite its vast potential promise, today, IoT still works in silos with an experience which is not unified across different environments. For example, smart home devices do not easily pair with hubs or apps, IoT features in cars are locked to certain providers. Nevertheless, key players such as Samsung, Apple, Google, Microsoft, Alibaba, and Amazon are committed to advancing interoperability to deliver a unified consumer experience. However, in the home or at the office, or from transport to retail to healthcare, there remains a huge amount of untapped potential in the application of IoT. Yet, as we will see in this report, driven by the increasingly digitised world we inhabit, a seamless, secure and constantly connected IoT experience is viewed as critical. What’s more, consumers expect to see this by 2030 everywhere in their lives, with a wide array of use cases at home, at work, outside, for healthcare, automotive services and commercial drones.

But it doesn’t stop there – consumers also visualize use cases for emerging technologies including artificial intelligence (AI) and automatic authentication methods based on behavioural biometrics. For all of these, they expect a fluid, personalized and unified experience providing continuity of services, together with the all-important security and privacy assurances. No easy task for organizations to fulfil.
Key consumer requirements must be met in order to enable the enormous potential of IoT, with significant security barriers to knock down on the way. Most pressingly for over half, are concerns about a lack of privacy (54%) and the threat of unauthorized parties controlling IoT devices (51%). With high profile data breaches seemingly an ever-present story in the media, unsurprisingly security tends to be at the forefront of the consumer mind in all aspects of IoT and emerging technologies – for example, consumers are putting security use cases for robots/drones before leisure purposes, and they want smart automotive services that they can trust and control. Essentially, the growth of connected objects, also involves the growth of potential security risks. Delegating security to a recognized leader in this field is a preferred method for consumers in order to overcome this problem. With greater trust comes greater acceptance, but as we will see in this report security must go hand-in-hand with convenience in order to successfully deliver the seamless experiences that consumers demand.

As we will go on to see, we also observed some regional differences, where fast emerging countries, such as China and Brazil seem to be adopting new technologies more rapidly, with enthusiasm for this being much higher than other countries, especially European countries such as Germany. This may be because the uptake of connected objects is developing much faster in these emerging countries, which in turn could result in them being the most advanced in the future regarding these new technologies.

The first step to properly meeting these changing consumer expectations is to properly understand them. The key findings from this survey aim to provide valuable insights to those involved in the ever evolving IoT ecosystem on what to address. Understanding these expectations offers the opportunity to unlock the full potential of IoT devices and related smart services that can be developed and offered to customers. Without doubt, the key players who can be first to harness the power of IoT and provide the best user experience, with a guarantee of security and privacy will lead the connected world.

To explore this in more detail, this survey investigates:

- How IoT will impact lives in 2030
- The level of connectivity and seamless experience that consumers expect from IoT
- What consumers demand from IoT for a range of technologies, including their level of acceptance and trust
- The security fears attached to IoT devices, including the level of privacy consumers expect and how much control they want to have over IoT devices by 2030

Scope of research/methodology

The research on which this report is based was conducted in April and May 2018. Interviews were conducted with 2,500 consumers aged 18 years old or over, across a range of countries:

<table>
<thead>
<tr>
<th>Country</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>500</td>
</tr>
<tr>
<td>China</td>
<td>500</td>
</tr>
<tr>
<td>UK</td>
<td>300</td>
</tr>
<tr>
<td>France</td>
<td>300</td>
</tr>
<tr>
<td>Germany</td>
<td>300</td>
</tr>
<tr>
<td>Brazil</td>
<td>300</td>
</tr>
<tr>
<td>Japan</td>
<td>300</td>
</tr>
<tr>
<td>Total</td>
<td>2,500</td>
</tr>
</tbody>
</table>

Interviews were conducted using online interviewing using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate. Unless otherwise indicated, the results discussed are based on the total sample.
The ideal IoT experience in 2030: a day in the life

By 2030, consumers would like IoT to be in all aspects of their day, including...

At home, in the morning...

- When I wake up, the wall in front of me shows the morning news based on my favourite headlines and day ahead, say 39%
- My fridge suggests a menu for my dinner in the evening, state 42%
- When I leave home, the temperature lowers to avoid wasting energy, cite 63%

At work, during the day...

- My computer/workstation starts up before I get to the office, controlled via my smartphone, report 43%
- My voice assistant sorts through my emails and pulls out urgent tasks for the day, state 40%
- The car park at work reserves a space for my car when it knows I am on my way to work, say 41%

Out and about, during the day...

- Walking along the street, a public terminal shows me where my favourite shops are nearby, report 30%
- When I have finished shopping, everything is automatically and securely paid as I walk out the shop, say 45%
The ideal IoT experience in 2030: a day in the life

Using AI technologies in daily life...

It will monitor my health and fitness e.g. it will recommend what I should eat and how much exercise I should do that day, taking my day schedule into account, report **48%**

**AI will assist me when I go outside**

e.g. advising me on the weather, planning my route for me, say **44%**

Using silent authentication in daily life – which locations?

**47%** would like to see this in banks e.g. being able to apply for finance services/access my account without carrying identification

**43%** say in the workplace/office e.g. entering the building without needing to be checked

**47%** would like this in airports e.g. going through passport control
By 2030, consumers anticipate an IoT experience that is omnipresent, seamless and personalized...

> The majority would like to see IoT perform a range of day-to-day tasks outside and be used for smart home services (86%), smart healthcare services (79%) and/or smart automotive services (78%) by 2030.

> It’s important that in every aspect of life, the IoT experience is seamless, with around eight in ten (79%) expecting this experience by 2030, where their house, car, phone and more can all ‘talk’ to each other.

> What’s more, they’re increasingly open to the benefits of emerging technologies such as AI and silent authentication (where a human is authenticated by intelligent systems, including machine learning, in a transparent way. This is done by the person being authenticated by multiple channels, such as behavior, habits, geolocation, tone of voice, body language etc.)...

> Personalization is also an important factor, with over half (56%) of consumers saying that they will improve the way they will authenticate themselves to services if they envisage IoT increasing between now and 2030.

> Over six in ten (62%) consumers say that silent authentication is critical or important to them, in order to have personalized services, which could explain why most (62%) are accepting of this technology.

> And this isn’t the only emerging technology they accept - approaching six in ten (57%) have a high level of acceptance in artificial intelligence (AI) and an even bigger proportion believe AI will positively impact them as a part of society by 2030.
Summary of key findings

However, trust remains a key hurdle to overcome if consumers are to be completely accepting of these new and emerging technologies and as such, most are willing to pay for guaranteed security...

> There are a range of security fears consumers have relating to IoT devices, with over six in ten (62%) expecting increased concerns over their privacy as a result of IoT increasing. A slightly smaller proportion fear unauthorized parties controlling their devices (51%) and/or a lack of control over their personal data. The current IoT ecosystem needs to address these fears whilst consumers need more education and reassurance around how their data is protected.

> It is clear that consumers recognize how crucial IoT security is, with nearly all (95%) deeming the security of IoT devices to be important and a well established company specialized in security (28%) being among the best positioned to protect their data on their IoT devices.

> And with around two thirds (64%) expressing they’d pay a premium for a guarantee of security on IoT devices, consumers will do what they can to reduce the security fears that they have.

---

**I will have increased concerns over my privacy as a result of IoT increasing, state 62%**

**51% of consumers fear unauthorized parties controlling their IoT devices**

**The security of IoT devices is important, say 95%**

**I would be willing to pay a premium for a guarantee of security on IoT devices, agree 64%**

---

Provided that these consumer expectations and criteria are met, IoT and related services will expand at their full potential in 2030.
IoT is on the rise, and consumers are excited to see what this will bring to their life. The majority (85%) expect IoT to grow from now to 2030, with over three quarters (78%) anticipating their life improving as a result.

But above anything else comes security. For over half of consumers, improving the way they will authenticate themselves to services is an anticipated benefit, highlighting a desire for a more personalized, seamless and secure IoT experience by 2030.

Having constant communication between people and objects is also expected to add to this experience because more than four in ten say that IoT rising will improve communication (48%) and/or make it more likely that they will have constant connectivity (43%). In fact, demonstrating the widespread potential benefits that consumers see from IoT in 2030, on average they anticipate four ways it could improve their lives – from the authentication and communication benefits already seen, to helping them make decisions, improving their health and beyond.

However, organizations within the IoT ecosystem need to take action for consumer IoT adoption, in order to address hurdles. Security fears are causing some consumers to feel that IoT growing will make their lives worse, which will ultimately result in them not experiencing the full potential of IoT. The main fears are increased concern over privacy (62%) and/or having less control over their life (50%).

But it doesn’t end there – over four in ten (42%) fear their life becoming more complex/confusing, suggesting IoT needs to be a fluid experience. This isn’t the case today, with IoT still stuck working in silos in many different areas, at home or in the car. It’s clear that IoT still has a long way to go until it meets the needs of the ideal consumer experience, as we will explore now.
For IoT to truly become key to consumers, it needs to fit around, and enhance, their daily lives – a seamless experience is crucial. By 2030, the vast majority (79%) of consumers expect this, where their house, car, phone etc. can all ‘talk’ to each other. Those from fast emerging countries tend to be the most enthusiastic about this experience, with over nine in ten expecting a seamless experience from China (94%) and Brazil (91%), compared to a lower proportion from the more developed countries but the trend is however the same. For instance, six in ten (60%) from Germany expect this experience, which is lower than any other region surveyed and may be due to sensitivity towards data protection in this country, which a seamless experience may threaten if not done securely. In spite of this, it is the majority from all countries who expect this, showing us how crucial being ‘seamless’ is to the IoT experience.

“I expect a seamless IoT experience by 2030, state 79%.”

This ties to the ways future IoT device owners expect to control their IoT devices by 2030. In line with consumer demands for security that is strong yet seamless, there is an ever-growing shift from the more traditional PIN/password commonly used today to an expected automatic, more convenient and personalized experience by 2030.

The main ways consumers expect to control their device in 2030 is through automatic (19%) or facial recognition (18%).

Only 6% plan to control their device through a PIN/password, while the most common method is through automatic or facial recognition, lessening the need for them to have to intervene manually and in turn providing a much more streamlined process. Many of us now expect these technologies in the palm of our hand. The increasing use of biometrics in mobile phones could be an explanation for this trend – normalizing it to authenticate and secure our most precious content and data.

Interestingly, region differences and preferences emerge which organizations must pay attention to. Consumers from Germany most commonly, compared to other surveyed countries, want to control their IoT device by 2030 through a fingerprint detector (28%), a method that is increasingly the norm today, and are least likely to want to through facial recognition (12%). Again, this may be due to sensitivity towards data protection and privacy, with a perception of a fingerprint detector giving them more control. Those in the UK (9%) and US (10%) are least likely to look to automatic recognition as a preferred control method, and in turn are among the more likely to retain some faith in pin/passwords (9% and 13% respectively). This contrasts with those from China who are much more likely than any other country, to want to control their device through automatic recognition (33%), and those from Japan who most commonly want to through facial (25%) or voice (22%) recognition. These are two countries with a particular thirst for new technology adoption.
Given a seamless and connected IoT experience is so vital, it is no surprise that consumers expect a more seamless connection with other connected objects (48%) from 5G by 2030. To support this, having greater coverage (57%) and/or an extended battery life for lower power IoT devices are also expectations of consumers from a 5G experience, which will allow for the all-important continuity of services. What’s more, automated and intelligent technologies such as robots/drones are increasingly accepted as a future part of society, with consumers reporting four important use cases for these, on average.

"I see search and rescue as the most important use case for robots/drones, say 63.""

They are most hopeful about this technology being used for search and rescue, security purposes and/or inspection purposes than simply for hobbyist/leisure purposes (20%). Clearly a feeling of safety and security from robots/drones is evident, together with the high level of trust that consumers have in those technologies, but such technologies are more likely to be seen as providing practical benefits as opposed to being purely for pleasure purposes.

Which of the following do you see as important use cases for robots/drones?

- Search and rescue: 63%
- Security purposes: 54%
- Inspection purposes: 47%
- Exploration: 47%
- Healthcare: 46%
- Transport/delivery: 43%
- Education/learning: 35%
- Purely for hobby purposes: 20%
- Don’t know: 5%
- I don’t think there are any important use cases for robots/drones: 5%

Which of the above do you see as important use cases for robots/drones?, asked to all respondents (2,500)
2: The future of IoT and consumer experience

IoT devices and smart services

A central area that technology continues to expand into our lives is in the home and looking ahead consumers would like IoT devices to do many different things in the home by 2030, particularly to increase comfort. Automatic temperature adjustments are most desired, where consumers expect it to lower to avoid wasting energy when they leave the home (63%) and/or adjust to their body temperature (53%). But that’s not all – many would like their fridge to suggest a menu for their dinner in the evening and/or their coffee machine to automatically make coffee for them at certain points of the day. This extends to when they go outside too, particularly when going shopping. Expectations of their IoT device automatically and securely paying for their shopping as they walk out the shop and/or their fridge telling them what shopping list to follow. Consumers are accepting of the futuristic capabilities of IoT in the home and beyond, adding to the seamless life experience they expect from IoT by 2030.

Furthermore, IoT devices should make work more efficient and save time for employed consumers, with common future anticipation of these devices being able to start up their computer before they get to the office (43%), their work car park reserving them a space before they arrive and/or their voice assistant sorting through their emails and pulling out urgent tasks for the day.

Smart services are also demanded by consumers, with the majority wanting to use smart home services (86%), smart healthcare services (79%) and/or smart automotive services (78%) by 2030. All important areas of day-to-day life that consumers increasingly see technology playing an important role in enhancing.

Starting in the home, smart security [59%] and/or smart meters are most desired for use by 2030, which similar to the important use cases for robots/drones we saw earlier, highlights how security remains the top priority for consumers, especially in the comfort of their own home. When it comes to health, consumers want more assistance and support by 2030 through wearable healthcare devices, telehealth and/or Ambient Assisted Living. And for smart automotive services, consumers would generally prefer to own their car, as opposed to rent it, with approaching four in ten wanting to use autonomous cars, as opposed to around a quarter with a desire for mobility-as-a-service. This desire could link to the fear we’ve seen previously around a lack of control – owning a car as opposed to renting would perhaps eliminate this concern for many.

All of these desires highlight how, in the future, consumers visualize IoT being omnipresent in their lives – at home, at work, in cars and outside.
Artificial Intelligence (AI)

AI has the potential to change my life for the better, agree 71%.

The seemingly unstoppable rise of artificial intelligence technology instils in us a mixture of emotions given its potential capabilities, however encouragingly, most consumers do believe that it has the potential to change their lives for the better (71%), with those from countries such as China (95%) and Brazil (85%) being most enthusiastic about this, compared to a much lower proportion from European nations such as France (59%) and Germany (56%).

This may be because of the regional differences we have seen in the anticipation of a seamless IoT experience, which AI could contribute to. In fact, those from Europe are generally less likely to be optimistic about the impact of AI, while those from Japan are not far behind the emerging countries, possibly because of the highly computerized nature of this country. These regional nuances are an important element for organizations to consider when rolling out new AI-driven services – a one size fits all approach may not work everywhere.

Nonetheless, on a global level, most are very optimistic about what this change will involve. By 2030, 78% believe that AI will positively impact them as a part of society, with monitoring personal health and fitness being the most likely (48%) outcome. This makes it unsurprising that AI is highly accepted by many (57%) as consumers clearly want the improved quality of life that this technology is seen as potentially being able to bring.

Given the positivity we have seen that consumers from China and Brazil have in AI, it is no surprise that they are much more highly accepting of this, than those from developed countries. Trust may be the main cause of these differences.
Artificial Intelligence (AI)

AI scares me, admit 51%, possibly because of the low level of trust around having less privacy and feeling less safe and secure.

This fear is amplified by the fact around half (51%) admit that AI scares them – perhaps fuelled by what they read in the press and see on screen about AI’s potential power. So, despite most consumers seeing the value in AI and wanting it to play a bigger role in their life by 2030, they won’t experience the positive life impact of this until their security trust and confidence is built.

**AI fears and the negative impact on society**

- There will be less privacy: 50%
- There will be a reliance on AI rather than seeking to learn ourselves: 49%
- Humans will communicate less: 46%
- The will be increased job loss: 44%
- Security and safety of people will be of greater concern: 43%
- I don’t think Artificial Intelligence (AI) will negatively impact society by 2030: 5%
- Don’t know: 9%

How do you think Artificial Intelligence (AI) will negatively impact you as a part of society by 2030?, asked to all respondents (2,500)
Silent Authentication

Silent authentication is critical or important in order to have personalized services, say 62%.

In the ‘search for seamless’, consumers globally believe that silent authentication could play an important role in society in the future. Personalization is key, with silent authentication being critical or important in order to have personalized services for six in ten (60%) consumers, which could be the main cause of a global acceptance (62%) in this technology. The most likely reason these consumers accept silent authentication is because of greater convenience, while only slightly fewer say that they would accept due to improved ease and/or speed of access, suggesting they want a fluid experience. And such an experience is expected in various locations between now and 2030, and for different use cases including airports (47%), banks (47%) and/or railway stations (47%). This suggests an element of trust in silent authentication, given how security sensitive these preferred locations are.

However, organizations still have a long way to go until consumers are completely trusting of this technology, with concerns about it being very risky (66%), invading privacy (59%) and/or data being misused (55%). Consumers need educating on the security methods involved in silent authentication as well as reassurance that their data is protected to increase confidence and trust.

Reasons for accepting silent authentication

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greater convenience</td>
<td>44%</td>
</tr>
<tr>
<td>Decreases the likelihood of identity theft</td>
<td>44%</td>
</tr>
<tr>
<td>and fraud</td>
<td></td>
</tr>
<tr>
<td>Improved ease of access</td>
<td>39%</td>
</tr>
<tr>
<td>Speed of access</td>
<td>37%</td>
</tr>
<tr>
<td>Avoid the need for any kind of password</td>
<td>33%</td>
</tr>
<tr>
<td>More personalized experience</td>
<td>31%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>3%</td>
</tr>
</tbody>
</table>

Why would you be accepting of silent authentication?, asked to respondents who would be completely, very or somewhat accepting of silent authentication (1,547)
We’ve seen that security is a central tenet for consumers in all their technology adoption considerations and opinions, which leaves an important question open: who is best placed to provide it? Those who own IoT devices or who expect to by 2030 most often think that the device manufacturer (28%) or a well-established company specialized in security (28%) are best positioned to protect their data on their device(s).

This is encouraging to see that some consumers understand that a recognized leader in the field of security would be best suited. However, a significant proportion (26%) of all consumers wouldn’t trust anyone more than another or don’t know who they would trust with this information, suggesting they find it hard to find out who they should trust the most.

A well-established company specialized in security is among the best positioned to protect my data, say 28% of current/future IoT device owners.

Who do you think is best positioned to protect your data on the IoT devices you use or plan to use by 2030?

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>The device manufacturer (such as Samsung or Apple)</td>
<td>28%</td>
</tr>
<tr>
<td>A well-established company specialized in security</td>
<td>28%</td>
</tr>
<tr>
<td>The service provider (such as Google or Apple)</td>
<td>18%</td>
</tr>
<tr>
<td>The online retailer (such as Amazon or Alibaba)</td>
<td>10%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>8%</td>
</tr>
<tr>
<td>I don’t think anyone is best positioned</td>
<td>7%</td>
</tr>
</tbody>
</table>

Who do you think is best positioned to protect your data on the IoT devices you use or plan to use by 2030?, asked to respondents who own at least one IoT device currently, or who expect to by 2030 [1,895]

Educating consumers about their security capabilities is a key task for any organization wanting to be a success in IoT.
The security of IoT devices is important, say 95%.

Organizations need to prioritize building trust and reassuring consumers that they can trust someone with their data, especially with nearly all (95%) consumers deeming the security of IoT devices to be important. What’s more, organizations could lose custom or stop themselves gaining more with a large proportion (78%) of consumers saying security is a top three priority when buying an IoT device, even more so than the cost (67%).

Which of the below are the highest priority, when thinking about purchasing IoT device(s)?

Which of the above are the highest priority, when thinking about purchasing IoT device(s)?, showing the combination of responses ranked first, second and third, asked to all respondents (2,500)
IoT security is crucial, yet we’ve already seen some consumers don’t trust anyone with this, and to add to this, they fear a lack of privacy [54%], unauthorized parties controlling the devices [51%] and/or a lack of control over their personal data [50%].

“I fear a lack of privacy regarding IoT devices, say 54%.”

What fears do you have regarding IoT devices?

<table>
<thead>
<tr>
<th>Fear</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of privacy (e.g. personal data being leaked/not knowing where my data is going)</td>
<td>54%</td>
</tr>
<tr>
<td>Unauthorized parties controlling the devices (e.g. a hacker)</td>
<td>51%</td>
</tr>
<tr>
<td>High cost/expense</td>
<td>50%</td>
</tr>
<tr>
<td>Lack of control over my personal data (who has access to it etc)</td>
<td>50%</td>
</tr>
<tr>
<td>Lack of control over the device</td>
<td>39%</td>
</tr>
<tr>
<td>Lack of legal responsibility</td>
<td>31%</td>
</tr>
<tr>
<td>Lack of external regulation on how to secure devices</td>
<td>31%</td>
</tr>
<tr>
<td>Lack of customer service to solve any issues which may arise (e.g. security problems)</td>
<td>30%</td>
</tr>
<tr>
<td>Not having connectivity when it is required</td>
<td>26%</td>
</tr>
<tr>
<td>Finding the devices confusing/complicated</td>
<td>25%</td>
</tr>
<tr>
<td>Being unsure which would be best use to me</td>
<td>16%</td>
</tr>
<tr>
<td>Lack of personalization attached to the devices</td>
<td>14%</td>
</tr>
<tr>
<td>I have no fears regarding IoT devices</td>
<td>3%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>5%</td>
</tr>
</tbody>
</table>

What fears do you have regarding IoT devices? asked to all respondents (2,500)
What’s more, almost all (95%) IoT device owners [or future owners] have concerns relating to the personal data that is collected for IoT devices. Trust must be built in order to reassure consumers that their data isn’t being improperly used or disclosed and give them a sense of control and visibility over it. This may also explain why over half the proportion of consumers have a high level of trust in cars with drivers, compared to autonomous cars (70% vs. 37% respectively), potentially because they want to feel a sense of control over their car and have visibility over the security.

64% would be willing to pay a premium for a guarantee of security on IoT devices.

With all of the security fears tied to IoT devices that we have seen, consumers are potentially willing to do what they can to eliminate this, with around two thirds (64%) expressing that they would pay a premium for a guarantee of security on IoT devices. This presents a clear opportunity for organizations, opening up new revenue streams that are there to be unlocked.
For it to fulfil its potential, IoT must escape its current silos because consumers visualize a more seamless, personalized and connected IoT experience by 2030.

And this expectation is universal as it applies for a range of smart services everywhere in their lives - at home, outside, at work and for automotive services. What’s more, consumers accept a range of emerging technologies, with anticipations of AI changing their life for the better, silent authentication being important for personalized services and robots/drones being key for a range of security and safety purposes. To add to this, countries such as China and Brazil are more rapidly adopting these technologies, with enthusiasm being much higher than in other parts of the world, in particular in Europe. Nonetheless, on a global level, having a fluid, personalized and unified experience with continuity of services, together with security and privacy is critical for all of the technologies we explored.

However, organizations need to do more to educate and reassure consumers of their safety, security and privacy when using IoT devices, and create more visibility and control over their personal data, because their fear is high and level of trust needs to improve. We have seen that the security of IoT devices needs improving and is more important than the cost when consumers think about purchasing these, so those organizations that can move quickly to address these issues, will stand to both retain and gain custom. Among the most preferred delegation of security, according to consumers, is a recognized leader in the field of security. What’s more, to eliminate the security fears we’ve seen throughout, many are willing to pay a premium for a guarantee of security.

Essentially, the key players who provide the most seamless and personalized user experience, with a guarantee of security and privacy will lead the connected world. Those involved who can provide this will be at the forefront of the IoT ecosystem by 2030.
ABOUT GEMALTO

Gemalto (Euronext NL0000400653 GTO) is the global leader in digital security, with 2017 annual revenues of 3 billion and customers in over 180 countries. We bring trust to an increasingly connected world.

From secure software to biometrics and encryption, our technologies and services enable businesses and governments to authenticate identities and protect data so they stay safe and enable services in personal devices, connected objects, the cloud and in between.

Gemalto’s solutions are at the heart of modern life, from payment to enterprise security and the internet of things. We authenticate people, transactions and objects, encrypt data and create value for software – enabling our clients to deliver secure digital services for billions of individuals and things.

Our 15,000 employees operate out of 114 offices, 40 personalization and data centers, and 35 research and software development centers located in 47 countries.

For more information visit:
https://www.gemalto.com/iot
https://www.gemalto.com/iot/consumer-electronics

CONTRIBUTORS

Rémi de Fouchier
Vice President, Marketing Communications, Gemalto

Didier Benkoël-Adechy
Marketing Communications Manager, Gemalto

Emmanuel Legros
Head of Marketing IoT & Consumer Electronics, Gemalto

Florent Abat
Marketing Manager, IoT Consumer & Electronics / Commercial Drones, Gemalto

ABOUT VANSON BOURNE

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis, is founded upon rigorous research principles and our ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com