Five Things To Consider With Home Automation

Five Things To Consider With Home Automation

I've been dreaming about a home that knows my needs and habits and reacts to them simply by being. The idea of home automation and pushing a single button and my living room turns into a theater is just so cool. The future: That's where I want to live. Come on, you know when a movie comes out and it's about the future, you want to see all the crazy, cool inventions **(think Demolition Man and the three seashells)**.

On the other hand, I worry all the time about the cost of the future. Who's using my data and why does it seem like, if I talk about wanting something, it magically appears on my next web search? Am I so lazy I can't turn on a light or adjust a thermostat? Why does my Samsung TV have a microphone? That's weird. Not to be cliché, but, it's all very Orwellian.

I came across an article written by Gareth Stokes and Anita Basi. They are lawyers for a firm called DLA Piper. Perhaps you've heard of them? They are global and, from what I've read, pretty dern smart. The following is an excerpt from an article they wrote and a few comments from a guy who's not half as smart as the two authors, but likes to share his viewpoint anyway, *ME*.

Five Legal Challenges for Home Automation and the Internet of Things

So-called ‘homes of the future’ have been a recurring theme for more than 50 years in popular culture and the technology industry.

When Hanna-Barbera created The Jetsons cartoon in 1962, for example, they had some interesting ideas about what the world would look like in 2062. Fifty-four years later and some of those ideas don’t look so out of place; mobile phones, flat screen televisions and video calls are now all firmly established features of everyday life. And, while we haven’t managed to mass-produce flying cars and pneumatic tube transport (yet), big steps have been made towards making automation commonplace in our homes. *The Jetsons was one of my favorites. Funny how it always came on after The Flintstones.*

Modern technology provides the ability to control third-party smart devices through a single interface. In practice, this means that people can switch off lights, lock doors, turn down thermostats and close window blinds at the push of a button. This suggests that we are moving ever closer to a unified Internet of Things (IoT), with George Jetson’s space-age lifestyle beginning to look like an attainable reality. Inevitably, alongside the opportunities, there are a number of challenges in the sector, not least the difficulty in getting consumers to embrace smart devices.

Reliability

For home automation to succeed, developers must address concerns about the reliability of smart devices compared with traditional home products and equipment. If connected devices do not possess similar functionality to precursor products, they could create a new class of problems, such as how to ensure service continuity in the event of an unexpected breakdown or service failure.

Think about the transition from landline to mobile phone. How many peoples parents and grandparents kept that landline

active? How many are still active? The good news is that even if you decide to automate your entire home, there will still be a few switches that will be put in place as a failsafe.

A large-scale service outage is one thing, but a connected device or home automation vendor is also at the mercy of the consumer's broadband connection.

To be fair, as of May 31, 2017, 25% of homes in the United States have the gold standard of residential internet connection, FTTH or Fiber to Home according to broadbandnow.com. Click here to learn more. This number is expected to double by 2022.

If your product cannot fall back to some lower standard of useful functionality when an internet connection is unavailable, the consumer's valuation of your product will be harmed every time their internet connection has problems. This creates a large third-party dependency for smart device companies.

SECURITY

Before consumers put their faith in smart home security systems and home automation, they need to be reassured that no malicious parties will be able to hack into their smart home systems, potentially giving thieves and vandals access to their data or even the ability physically to enter their homes.

With an increasing number of home automation devices, including microphones, cameras and other monitoring technologies, a compromised home automation set-up could allow cyber criminals to record residents in the intimacy of their homes.

Additionally, compromised IoT devices with weak security or set-up processes that allow consumers to use the devices with default passwords unchanged have recently been used as part of

huge distributed denial-of-service (DDoS) attacks, programs which take servers offline by overwhelming them with inbound data.

Implementing strong security measures is essential for IoT vendors if their products are not to become a vector for spying, blackmail, DDoS attacks or worse. Developers need to consider solutions that force default passwords to be changed, and implement end-to-end encryption between devices.

Fear tactics are not my style. Everyone is aware of cybercrime. If not, you shouldn't worry. You're the wrong demographic.

Electricians and IT professionals are going to be best friends in the coming years. ***Check out this survey from Klein Tools.***

Having experience in both fields, I know there are solutions to protecting your IoT life, such as VPN's and Firewalls. Talking through and finding solutions to Cybercrime is a better alternative than allowing fear to keep you living in the Stone Age. Talk to an industry professional.

DATA COLLECTION AND USE

Many connected home and smart products rely on value propositions that are in part about new functionality, and in part about the 'smarter' use of resources. In order to achieve this, data flows between the devices and servers operated by the device providers, between devices, and to and from the consumer's smartphone or computer.

This creates opportunities to collect data that can be used to improve the service, or be analyzed by marketers to learn about consumers' habits to build and grow existing relationships.

Much of the information being generated and collected is 'personal data' within the meaning of Directive 95/46/EC, and

with the General Data Protection Regulation (GDPR) set to come into force in the EU on 25 May 2018, any businesses looking to take advantage of these opportunities should keep data privacy at the top of their agendas.

Even if the systems are not hacked by malicious third parties, users and consumers need to be reassured that the vendors supplying these products and services are themselves trustworthy.

Vendors need to see compliance with data protection laws as a value differentiator when developing their product offerings and marketing strategies. Vendors that fail to do this will gradually lose out in an increasingly data and privacy conscious market.

This is a hard one for me. Convenience vs Intrusion. A product wants to make my life easier and market things to me that I have expressed interest in. Not bad. Having real time analysis of movement in my home. Bad. This is a line that either you are comfortable with or you're not. Not sure? What Browser do you use? This can tell you what level of concern you have.

DIGITAL TRANSFORMATION AND INTEGRATION

The evolving 'connected home' means that many related professions, such as locksmith, heating engineer and electrician, need to consider putting software at the heart of their businesses and transforming themselves into digital providers to keep up with the market.

These professionals still represent key intermediaries for consumer choices about major installation projects. Vendors that understand this, and provide software tools which can be deployed to interact with particular products, are more likely to benefit from the goodwill generated in the professional community.

Another factor to consider is standardization and the ability to connect to systems/devices from other manufacturers. Having APIs or other standards-based connectivity solutions that allow devices to control/be controlled by other devices can add significantly to the overall value proposition to the consumer.

This raises the question of which company owns particular standards for device interconnectivity. Where any partnerships with other device manufacturers, app developers or platform providers are to be considered, both parties should address and carefully document how any newly created intellectual property will be owned at the outset to avoid difficulties down the line.

Many products now have Hub's and Bridges that link different products. ***Another piece of good news: IoT is getting a common language****. Sorry for all the pop-ups on this site. Not my doing but it's valuable info.* ***Check out Radio Ra2 products here****.* ***Home Automation applications****.*

Liability

Solutions to smart device problems often come in the form of updates and patches, which aren't always completely reliable. Developers also need to bear in mind that not all users will download updates as they become available, leading to 'version lag' as devices continue to run older software.

In addition to creating support challenges for vendors, this could leave devices vulnerable to attack. All of this creates a complex situation from a product liability perspective, as the device being used at any given point may function very differently to the device the consumer first bought.

Since many connected devices require an ongoing service component from the vendor to function, the consumer-facing T&Cs associated with a service are one way for manufacturers to try to limit and exclude liability.

The effectiveness of this strategy will vary by jurisdiction, and the law is likely to step in to render exclusions or limitations invalid in jurisdictions with a more protective attitude to consumer rights.

Where the relevant manufacturer has partnered with another device manufacturer or platform provider, these kinds of liability issues can be addressed in the agreements that govern the commercial relationship.

In many cases, where manufacturers simply follow a published standard for device interaction, or use a documented public API, liabilities will be less clearly delineated, and vendors will have to proceed on the assumption that they may bear a substantial part of the risk even if there are extrinsic factors involved.

I like the idea that any company creating a product that is considered IoT should be responsible for updating and patching their products for a given period of time. If a security issue is found and not addressed within 30 days, said security issue should be freely advertised. No successful IoT based company is a one hit wonder. If your thermostat has a security flaw, patch it and let's keep moving.