



Internet of Things: How to Avoid Short-Term Errors and Ensure Lasting Adoption

Larry Downes

KEYWORDS

*IoT Strategy,
Big Bang Disruption,
Shark Fin Adoption Model*

THE AUTHOR

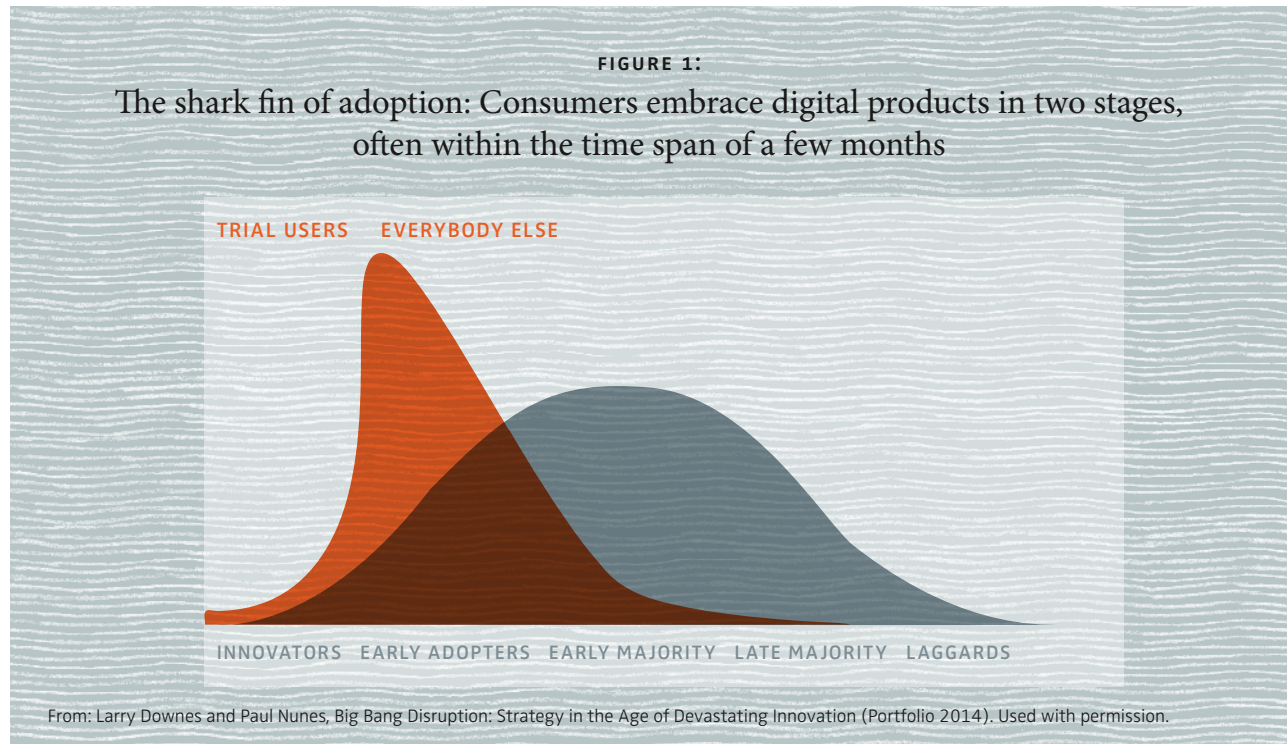
Larry Downes
Project Director,
Georgetown Center for
Business and Public Policy,
Washington, D.C., USA,
larry@larrydownes.com

The Internet of Things is at risk of becoming a victim of its own popularity

/// Today, the IoT market is generating \$200 billion in revenue, a number expected to triple in the next 10 years. But a rush to market by developers of consumer IoT products and services has been accompanied by shortcuts in design, particularly in information security, usability and branding. Several embarrassing and highly public data breaches have left buyers increasingly wary of embracing smart technology, slowing market adoption for products both good and otherwise.

These early market failures must be corrected, and quickly, if the IoT is to reach its full potential. Soon, up to a trillion items in everyday will become “smart” devices, allowing them to send and receive data over the global Internet. Machine-to-machine applications will help seniors age in their own homes and make possible truly autonomous vehicles. For manufacturing, agriculture and energy, among other verticals, IoT technology promises vast improvements in supply chain efficiency and sustainability.

Consumer surveys over the last few years, however, reveal slower-than-expected adoption of IoT solutions. Stories of hacked baby monitors and connected toys, video cameras taken over by botnets and fitness trackers revealing the locations of secured military installations, coupled with a lack of clear user value propositions, have generated skepticism that IoT applications are really ready for mass markets or, indeed, if they ever will be.



“Big bang disruption” demands new marketing strategies /// These marketing problems are a side-effect of what I have termed “big bang disruption,” where disruptive innovations, following a short period of failed market experiments, achieve wide-scale adoption quickly – sometimes in a matter of weeks. Today’s disruptors have replaced the classic bell-shaped model of adoption famously described by Everett Rogers with a distorted curve that resembles, appropriately enough, a shark fin. While adoption followed five fairly predictable stages (see figure 1) in the old economy, the adoption of digital products has shrunk to two stages and is happening much faster. Sometimes the rise and fall happen within weeks only – as happened with Pokémon Go in summer 2016.

As in other recent examples of big bang disruption, the IoT’s shark fin is being driven by a combination of factors, including rapidly falling prices (and sizes) for sensors, wireless receivers and transmitters, semiconductors and other component parts.

Coupled with an increasingly ubiquitous platform of high-speed broadband access and cloud-based services, new prod-

»
While adoption followed five fairly predictable stages in the old economy, the adoption of digital products has shrunk to two stages and is happening much faster.
«

ucts can be launched quickly and cheaply. And with social media empowering consumer-to-consumer marketing in real-time, buyers sort the winners from the losers immediately, driving short-lived but dramatic winner-take-all success for the lucky few.

The pressure of delivering products in hyper-competitive markets, however, often leads developers to ignore basic data management precautions, along with a failure to devote adequate resources to other marketing imperatives.

Marketing imperatives for the Internet of Things

/// That's precisely what's happening for the IoT – damaging a valuable new market for everyone. So to assure these short-term errors don't cause long-term damage, developers must adopt five related strategies that have been central to successful deployment of earlier big bang disruptors.

Converge on a single set of standards /// As is typical with emerging technologies, every Internet of Things developer hopes to establish itself as the industry standard for interactions with other networks and other products. Competing industry groups have also sprouted up, each offering to eliminate incompatibilities by offering an open, neutral set of communications and data exchange rules anyone can follow. IoT standards wars are taking place for everything from devices finding each other and coordinating activities, establishing low-power wide-area networks, and sharing data in standard formats. Major hardware and software vendors, including Qualcomm, Intel, Google and Amazon are offering combinations of proprietary and open solutions, along with consortiums including the Zigbee Alliance and Z-Wave.

»

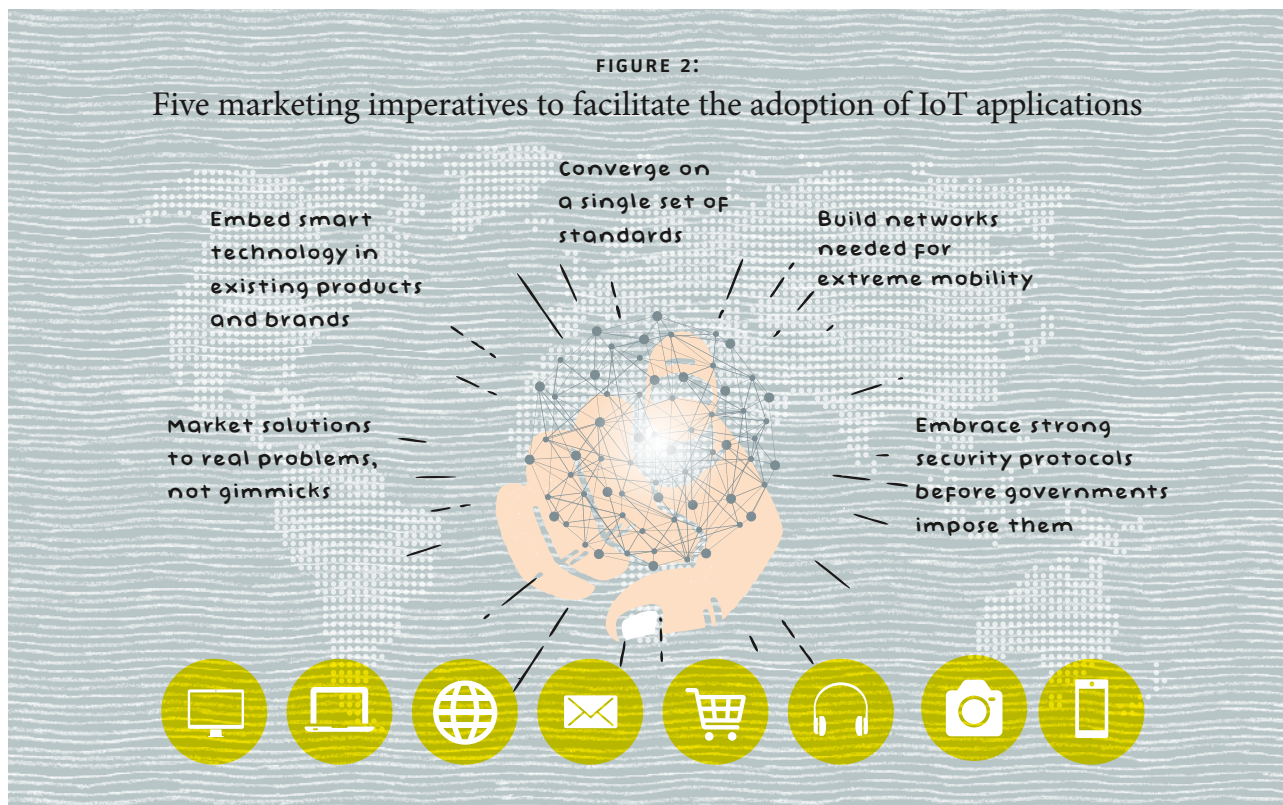
The pressure of delivering products in hyper-competitive markets, often leads developers to ignore basic data management precautions.

«

Some Internet of Things vendors are now building products that follow everyone's standards, while others are leaving the problem to third-party developers. The standards war will undoubtedly be resolved, but in the interim consumers are understandably hesitant to make big investments in new systems.

FIGURE 2:

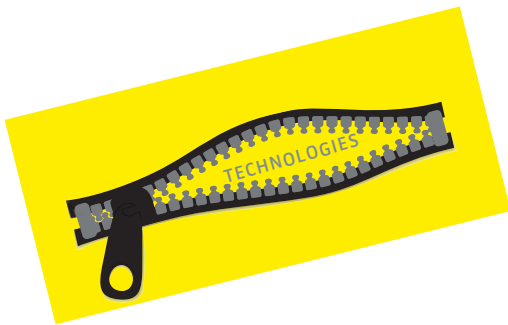
Five marketing imperatives to facilitate the adoption of IoT applications



>>

To work for all consumers, technologies that transform markets must be integrated into existing solutions from trusted brands and become invisible.

<<



Build networks needed for extreme mobility /// Internet of Things devices may never have to communicate large volumes of data, but the sheer number of connected items and the need for constant interaction for many of them can't be supported even with today's fastest mobile networks.

That's one reason mobile providers and their partners are investing billions in next-generation 5G networks, which will increase network speed and capacity by orders of magnitude. The 5G architecture optimizes performance for both the close quarters of your home and the potential free range of autonomous vehicles on the road and in the air.

5G standards groups are still working on the details, but network operators and their hardware partners are already testing equipment that can deliver speeds that are dramatically faster and more reliably than existing mobile technology. In the United States, both Verizon and AT&T are already conducting 5G tests. The new networks, however, require more and different ranges of radio frequencies, which only regulators can allocate. It may not be until 2020 that robust and ubiquitous 5G service is in place.

Embed smart technology in existing products and brands

/// For IoT products that integrate deeply into the consumer's daily life and which collect sensitive data, applications must be integrated into existing solutions from trusted brands. Since 2015, for example, fitness technology leader Under Armour has invested heavily in the nascent Internet of Things. Its Connected Fitness platform allows customers to import tracking data from a wide range of devices and third-party products, including those of Under Armour's competitors, into a single dashboard and a series of apps.

Or consider IoT technology aimed at improving sleep. Early efforts required users to remember to wear separate devices that were uncomfortable to sleep with or install extra equipment under an existing "dumb" mattress.

Compare that to products now being marketed by Sleep Number as part of its "Smart Bed" line. Sleep Number, a familiar brand already associated with technology-based innovation, was the first major industry player to build sensors right into the mattress.

To work for all consumers, technologies that transform markets must become similarly invisible. Ironically, the more disruptive the technology is, the sooner it needs to disappear.

Embrace strong security protocols before governments impose them ///

IoT products will collect potentially sensitive personal information about its users, heightening growing security concerns for digital products and services generally. To avoid consumer resistance and the potential intervention of regulators who may unintentionally slow or skew the trajectory of IoT adoption, manufacturers must quickly coalesce around industry best practices for data collection, analysis and storage.

So far, many smart devices have proven to be pretty stupid; more than a few early products released with inadequate protection, as noted, have experienced embarrassing security breaches. The Federal Trade Commission and other regulators have already brought enforcement actions under consumer protection laws against several vendors who failed to live up to security promises. More broadly, lawmakers are circling the emerging industry, threatening preemptive regulation, specific rules and invasive oversight.

An industry-led alternative should be quickly developed. It could come from a combination of general standards bodies,

including the International Organization for Standards, and more targeted efforts, such as IoT best practices recently proposed by the Broadband Internet Technology Advisory Group. Policymakers should likewise be careful about regulating too soon or too heavily. Overreaction to what may be simply growing pains for the Internet of Things may unintentionally delay both the development and adoption of technology that will actually improve the safety and security of activities, such as transportation, that today rely on highly-fallible human operators.

Market solutions to real problems, not gimmicks – If IoT developers want to ride the wave of a big bang shark fin, their products must do more than simply replace existing and still-working items in the consumer's life. They must do so in a way that adds new functions and new applications that existing technology can't possibly duplicate.

Up until now, according to Donna L. Hoffman and Thomas P. Novak, companies pitching IoT gear have focused on specific applications, fragmenting the overall market. A smart refrigerator, a connected toothbrush or an intelligent thermostat may each be worth the cost and hassle of adoption for some consumers. But individually they don't deliver on the promise of a connected life. Standing alone, they're just gadgets. "The key to smart home marketing is to view the smart home as a complex dynamic system," write Hoffman and Novak. To jump-start mass adoption, marketers must instead "focus on communicating the value proposition inherent in experience; current approaches may actually be underselling the smart home."

Developers, in other words, must provide solutions to actual consumer problems – which means, for one thing, performing the kind of market research necessary to know what those problems are.

In home security, for example, most early offerings were simply "smart" door locks that could be opened and closed remotely using smartphones and tablets as the controller. Compare these limited-interest products to offerings from Piper, Comcast and others, which integrate digital cameras, motion sensors and wireless notifications to offer a more complete home security solution.

Get ready for the bang /// There is plenty of incentive for entrepreneurs to adapt these strategies. The IoT market, properly configured, could grow to \$2 trillion by 2022. As these issues are resolved, the Internet of Things will experience the kind of dramatic takeoff that followed the introduction a few years ago of smartphones that users actually enjoyed owning.

./

FURTHER READING

Downes, Larry and Nunes, Paul (2013):

"Big Bang Disruption," Harvard Business Review (March)
<https://hbr.org/2013/03/big-bang-disruption>

Hoffman, Donna L. and Novak, Thomas P. (2016):

"How to Market the Smart Home,"

The Center for the Connected Consumer,
<https://postsocialgwu.files.wordpress.com/2017/01/hoffman-and-novak-how-to-market-the-smart-home-1-15-2016.pdf>

Accenture (2016):

"Igniting Growth in Consumer Technology,"
https://www.accenture.com/_acnmedia/PDF-3/Accenture-Igniting-Growth-in-Consumer-Technology.pdf#zoom=50

Broadband Internet Technical Advisory Group:

"Internet of Things Privacy and Security Recommendations," Nov. 2016

[https://www.bitag.org/documents/BITAG_Report__Internet_of_Things_\(IoT\)_Security_and_Privacy_Recommendations.pdf](https://www.bitag.org/documents/BITAG_Report__Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf)

