



Ebook:

# THE FUTURE OF THE INTERNET IS HERE, IT'S JUST NOT EVENLY DISTRIBUTED

(With Apologies to William Gibson)

ORACLE® + Dyn

 [dyn.com](https://dyn.com)

 603 668 4998

 @dyn

## Ebook:

# The Future of the Internet is Here, It's Just Not Evenly Distributed (With Apologies to William Gibson)

How the internet is changing  
and what that means for your business.

## Introduction

As more and more businesses migrate key applications and infrastructure to the cloud, the performance of the Internet will play a larger role in their success. It is ironic, however, that as many enterprises begin to rely on the Internet, they will find that it is undergoing a dramatic transformation. In fact, there are some trends that we see today that are harbingers of the way the Internet may develop in the next few years. I want to be clear that I'm not predicting the future here. After all, as William Gibson famously said, "The future is already here; it's just not very evenly distributed." What I want to address are things I already see happening that I believe will become important elements in how the Internet develops. Additionally, I will discuss what businesses can do to thrive amidst these developments.

There are three main trends that are converging to shape the future of the Internet. I'll begin with the so-called "second enclosure." Then I'll turn to the corresponding "end of privacy" and the way that information control has in many cases already been lost. The third is the burgeoning Internet of Things (IoT), which can be viewed as an experiment in which we connect as many unmanaged, nonsecure devices as possible to the Internet and see what happens.



All of these trends encourage a kind of interest on the part of regulators that could very much change the nature of the Internet itself. The Internet's nature does not lend itself to regulation, and yet governments are displaying considerable interest in developing such regulations.

If you are a business that depends on the Internet, there are both near-term and longer-term things you can do. On the technical front, you can adopt a strategy based on Internet performance. You need to understand how your business exists in the Internet and how global network events might affect that business. This includes understanding peering relationships and their impact on the performance of your Internet operations. It also means being prepared for brand damaging events like DDoS attacks. At the same time, on the corporate strategy front, you must ensure you are promoting and supporting safe and sensible Internet operations, to ensure that regulation does not break the virtuous circle of innovation that the Internet has provided.

## The Second Enclosure

In the 18th century, the British countryside was transformed. Formerly open areas, which had been treated as common land, were turned into private preserves controlled by a landowner. A great deal of modern property law throughout the world rests on the foundation of this "first" enclosure.

**James Boyle** has argued that the same thing is happening on the Internet. This second enclosure movement occurred initially as a legal assertion of rights of ownership over various kinds of intellectual property. Looking around at the Internet today, we can see the hallmarks of that sort of enclosure. Freewheeling conversations on Usenet groups, public mailing lists, and even blogs have gradually moved into controlled environments with terms of service that nobody reads but that give control to the corporation operating the environment (e.g., LinkedIn, Medium and Facebook). Large social media sites overwhelm the public web as a source of information. Even the **Canadian Broadcasting Corporation's Radio 1** service (which has no advertising) now urges listeners to visit their shows' Facebook pages. The Internet's tradition of permissionless innovation at the edge is being shut out by mediation:

apps on mobile devices mediate every interaction, narrow the user's options, and provide advantages to the vendor over the user. Privacy is a thing of the past. And control over innovation lies in the hands of the few corporations who make a killer app and control its API. These systems sure sound like walled gardens. Indeed, while they are often called "ecosystems," but that they are the opposite. Ecosystems grow and evolve on their own. These systems are carefully managed and tightly controlled. They are parks, not ecosystems.

This sort of enclosure undermines one of the most important reasons that the Internet has been so transformative: they take power away from consumers and vest it in either the operator of the service or, in the case of some ISPs (especially mobile operators) those who control the means of transmission. The traditions of the Internet press against this enclosure, but commercial interests press in favour of it. The open question is which of these pressures will be greater.

The irony is that, while near-term commercial interests press in favor of enclosure, the long-term interest presses the opposite way. In the Internet of Things market, for example, many early entries attempted to keep devices in closed systems: they used proprietary communication protocols, or they worked exclusively with one company's API, or they only worked when in communication with the manufacturer's servers. But while consumers may be willing to accept commercial lock-in for consumer electronics with a short life, they are unlikely to be willing to commit to one company's services for products like light switches, which are effectively lifetime purchases.

Similarly, nobody is going to buy a light bulb that won't work with other brands of light bulb -- do you even know what brand of light bulb you use? -- or one that won't work whenever the cable modem goes down. And nobody wants to have 300 apps in order to control the 300 devices in their house. As a consequence, interoperation standards need to emerge. Efforts like the **Internet of Things Semantic Interoperability Workshop** show that vendors recognize the value of interoperation. This kind of effort is late and adds complexity, but it shows people have remembered that it is supposed to be the Internet of Things, not just the internet of Things.

When designing new products and services that relate to the Internet, it is tempting to try to “own” the consumer, so that a competitor can’t draw them away. Investors’ appetite for “unicorns” especially encourages this approach. But the strategy restricts the growth of the overall market to the size achievable by a single company’s customer base. Reusing or establishing open APIs allows the potential market to grow even at the risk of having some potential customers using a different provider. The Internet’s period of explosive growth depended on such interoperable standards, so it seems wise to look to that strategy for similar future growth.

## The End of Privacy and the Loss of Information Control

Privacy and security are related but basically different problems on the network. They’re so tightly linked to one another in popular experience, however, that any practical policy must consider them as almost a single issue.

An important driver of privacy and security concerns comes from two related trends converging. The rise of “big data” means that privacy that used to come from the inaccessibility of data about everyone is gone. People are willing to give up this data about themselves in the interests of convenience, and there is little reason to suppose that the trend is going to reverse any time soon. Storage, computing processing power, and network interconnection are all getting cheaper. That suggests that privacy, as such, is going to have to be taken over by some new idea of privacy that is context-appropriate. This is almost certainly an area where the culture will need to adapt to the new technology, regardless of any regulations countries adopt. The all-seeing eye is here, and it is almost certainly undertaking its efforts with your explicit consent.

But the ability of people to put disparate sets of data together is made radically worse by truly woeful security practices around the handling of that data. Every day brings a new story of a data breach. Each ought to seem incredible; instead, we are numb from the

the number and scope of them. Despite greater regulation of data handling in Europe as compared to the United States, it is not clear whether there are fewer breaches there or whether the lack of a public reporting requirement just means we hear about them less often. The United States does not have an overarching data protection law, but many states require notification of consumers in the event of data breaches. In Europe, the Data Protection Directive (Directive 95/46/EC) is a very large framework covering individuals’ data, but the EU General Data Protection Regulation (Regulation 2016/679) was only finally settled in April of 2016.

These pressures are causing the protocol world to reduce the data that is available at any point in the network. Protocol developers are reducing the amount of data that could be “leaked” by any protocol exchange, and increasingly protocol messages are encrypted to reduce the ability to view the payload. But these attempts do not really work to preserve privacy and information control in the presence of very large cloud providers who necessarily see all the payloads and know who the users are.

For businesses, there are three things to consider for the future. The first is cost and uncoded liabilities. Home Depot, for instance, had a data breach that exposed data for just five months in 2014. The cash settlement alone was US\$13 million, and the total pretax gross expenses for the breach reported in May 2016 was US\$261 million. This may not sound like much for a multibillion-dollar company, but very few companies can afford to give back tens of millions of dollars at a time. And the history of corporate liability (particularly in the United States) suggests that these sorts of liabilities can be invisible for a long time until suddenly they come due at once. You should have a clear idea of your vulnerability to such costs due to data you have.

The second consideration is the real utility of the data in the first place. Peter Wayner’s classic *Translucent Databases* describes strategies to avoid problems with data, and the most important one is not to store something you do not really need. It is often better to analyze some data and store the analysis instead, because that technique prevents a potential intruder from getting data it can pass on. It also makes the

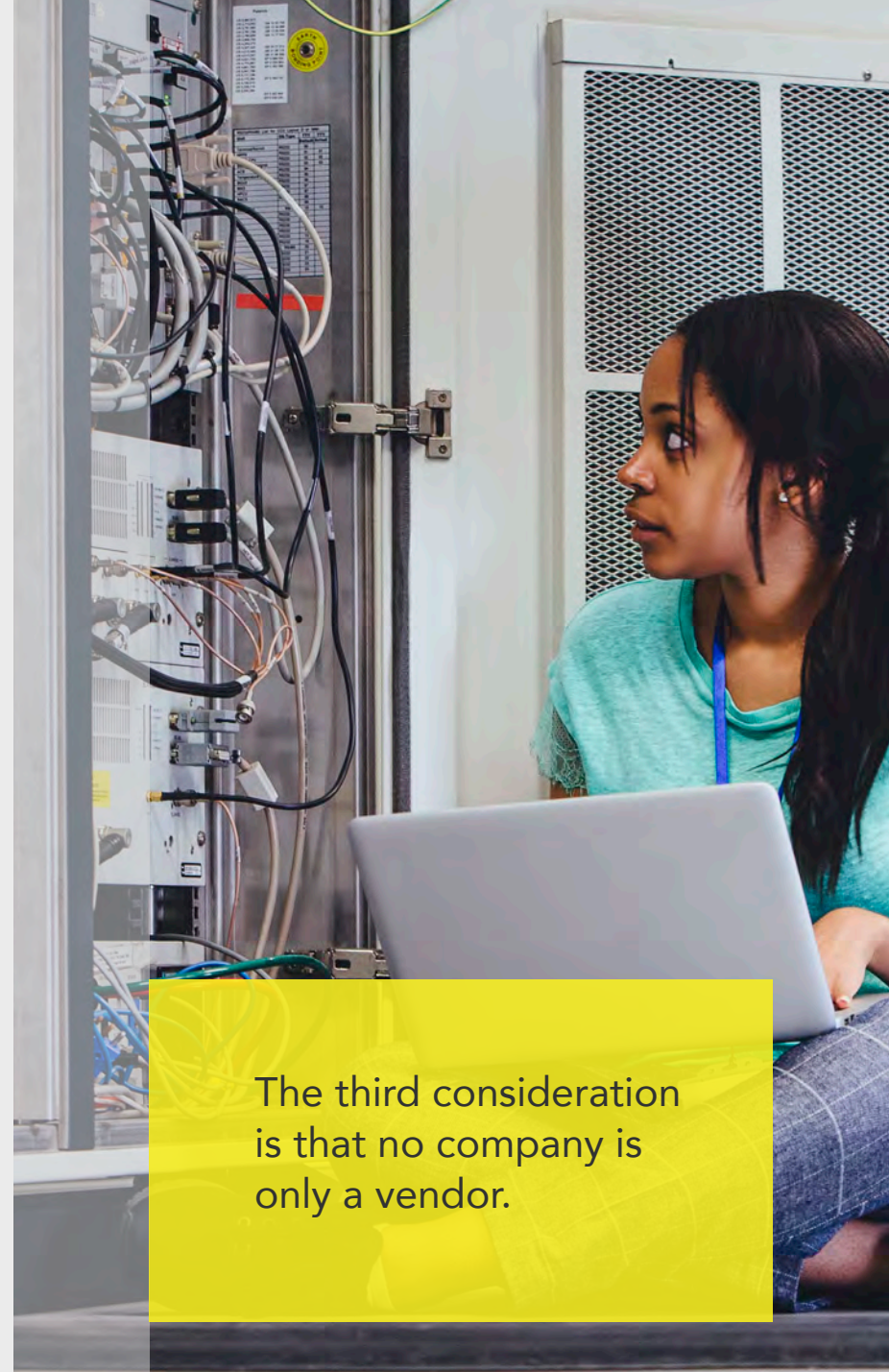
business more valuable, because the value lies not only in the data the business has but also what it can do with that data.

The third consideration is that no company is only a vendor. You consume from others, and those suppliers' handling of data exposes you to risk. Don't neglect these risks, because you don't want your supplier's bad day to be yours.

## The Internet of Things That Break

Both of the foregoing trends are made much worse by the way that so-called Internet of Things devices are being deployed. There are three issues here. First, the incentives for good security are exactly backwards: good security makes usability harder, and most of the "Things" in question are consumer devices with no user interface. So good security would cause user support problems, and so it's left out. Moreover, the commercial pressures to ship devices to market immediately are enormous, and therefore security issues are dealt with as an afterthought. Finally, the number of devices is quite a lot larger than the number of people, which means that the population of end points is exploding. But there is no "access control" to the Internet, and these enormous numbers of devices are mostly unmanaged, so the IoT becomes a big source of botnet participants.

There is a central threat here for companies that depend on the Internet. The historic pattern of attacks often involved spoofed traffic from botnets under the control of an attacker. The spoofed traffic was effective because of the way the Internet works, and there is no reason to suppose that old-fashioned, spoofing-based attacks are going to disappear. But the deployment of millions of devices on the Internet with poor security means that it becomes trivial for an attacker to assemble a new weapon: a network of thousands of devices that look just like a flash crowd. Really protecting against attacks like this will never be possible, because it would also "protect" against a sudden surge of sales or interest. So instead, managing Internet performance becomes more important than ever. Your infrastructure needs to be able to react faster than human speed, and to measure itself all the time so that emergencies are handled automatically, rather than being discovered by a complaint (often public) from an unhappy or lost customer.



The third consideration is that no company is only a vendor.

While all this is happening, IoT is altering the patterns of use of the Internet. Historically, the bulk of Internet traffic was destined at one end or the other for “eyeballs.” Even support pieces, like the DNS, had the underlying purpose of connecting a human to some service. But IoT devices talk to other machines, not to humans. This means that the pattern of traffic on the Internet will change as IoT devices begin to be a larger population. So, your measurements of the network need to be sophisticated and to reflect a deep understanding of the changes that are happening. On the Internet, performance management is not about hitting a static target. The target moves, and you need to as well.

Finally, the Things that we are connecting to the Internet, at least at the start, will mostly be things we already have: lights, security cameras, thermostats, water meters, electric meters, alarm systems, and so on. Devices like these were not invented as networked devices, and users’ mental model of them does not include networking -- even though the youngest among us are growing up in a world where everything is networked, and a product does not really work unless it is connected. In any case, the newly networked Things are very often otherwise subject to some sort of regulation. And that brings us to the attention from governments.

## Unsafe at Any Line Speed?

A little over 50 years ago, an enormous transformation in the automotive world began. Ralph Nader’s book *Unsafe at Any Speed* is today mostly famous for destroying the Chevrolet Corvair in North America. But its more lasting effect was to turn the United States, a country overwhelmingly the home of car culture, toward a regulatory regime of the automobile. As the automotive executive Bob Lutz said, the book had a “seminal effect” in ensuring that “there was definitely a role for government in automotive safety.”

Transformative technologies do not merely add something new to the existing cultures into which they are introduced. Because they are transformative, they conflict with those pre-existing cultures. For example, in the earliest part of the 20th century, the idea that

pedestrians needed to cross North American streets at well-regulated points, in deference to vehicular traffic, would have been laughable. By the 1920s, it had gained traction, particularly in Los Angeles. A cultural conflict was resolved, and the humans had to change their behavior to accommodate the new technology.

The Internet is another transformative technology: it is not only altering the way we live and work but, if you believe some authors, even the way we think. Any story about the future of the Internet is going to need to account for social interests similar to what the automotive industry faced, which brings us back to Nader’s statement about “new instruments of citizen action.”

The Internet’s peculiar structure makes it different from the automotive world. Since the Internet is a network of networks, the overall behavior of “the Internet” is the behavior of its constituent networks. But those networks may have the same property, and so on, which makes it very difficult if not impossible to know just whose behavior needs to be shaped. Moreover, since almost all the infrastructure is privately owned, in many countries it is tough to regulate the use of that infrastructure: your network, your rules. It is not like vehicular traffic: the majority of roads are publicly owned. Regulation is, of course, often possible where there are consumer relations or where some provider has a monopoly or near-monopoly for some service, but in general the lever of government regulation comes from the fact that it alone can permit or deny an action or business access to a good. The Internet is at bottom designed to avoid such choke points, so it resists easy regulation.


Moreover, the Internet protocols place no value on national boundaries. Since roughly all of the packet routing on the Internet today attempts to use the network-topologically shortest path, geography simply does not enter into consideration. The endpoints of any Internet-carried packet are, of course, in a place. But the path between those places is not predetermined. Indeed, the path must not be predetermined. For the Internet makes a reliable system out of unreliable parts -- that is very nearly the point of the Internet.

Its very resilience relies on being able to make use of different routes and to go around the things that are in the way. But this feature means that national regulation either won't work; or else it will actually damage the very thing being regulated, supposedly for the benefit of all.

Finally, it's important to remember the speed of change on the Internet, and to try to square that with regulatory regimes. One of the facts of networking is that there are many different ways to achieve a result. At the limits, there may be only two possible outcomes: that regulations end up protecting existing players at the expense of possible future competition; or else that regulations will not be effective at achieving what they want, because clever operators can find a way around the spirit of the regulation due to the plastic nature of internetworking. Neither of these outcomes does anything to promote "new instruments of citizen action." And this point also suggests part of the reason why international treaties are not the answer: the speed of a single country's regulator is unlikely to be increased in union with the speed of 192 other countries' regulators.

The only reasonable conclusion, then, is that network operators are going to have to figure out how to address public concerns, and to do that reliably and in a way that addresses the interests of consumers. It seems we need to imagine the alternative history, where the automotive companies invested significantly in safety, efficiency, and low pollution, exactly as Nader complained they would not do. At the time, car companies said consumers weren't interested. The question for the Internet industry is whether we will turn out to be interested in doing this. Because the alternative will be that the Internet will get government regulation, even if that turns out to damage the Internet in unpredictable ways.

For companies working on the Internet, all of this means building product and service plans in a way that addresses consumer concerns with the first three trends outlined above. Your company may not be affected by all of those trends, but it is almost certainly affected by one of them. A key goal is to maintain the ability to create new services at the edge of the network, without seeking anyone's permission. That is what has made the Internet an engine of explosive growth.



A key goal is to maintain the ability to create new services at the edge of the network, without seeking anyone's permission. That is what has made the Internet an engine of explosive growth.

## Your Users' Internet Experience Must Be in Your Hands

The plain fact is that nobody cares about your own users and customers except you. They have their own problems. So you must ensure that your users and customers -- current and potential -- get the experience they want and that you desire they get.

Both local and global events can affect you. To be in control of this, you need an Internet performance management strategy that ensures you know when something is affecting you, that responds to those events, and that ensures a good user experience without manual intervention. It is impossible to do this without measuring of the way the global Internet interacts with your services, and reacting to those measurements as the Internet swirls and changes around you. These can be large trends, like changes to the mix of devices and kinds of traffic. They can also be sharp, focused, and sudden changes, like DDoS attacks that look just like a flash crowd of interested customers. Your users won't care why things don't work, so you must have an Internet performance management strategy that keeps you in control.

By keeping an eye on the trends affecting Internet business, you can craft a strategy that ensures your continued growth.

A key part of that strategy involves ensuring that you always have additional options to ensure the control remains in your hands without destroying the profit in your products and services. Internet performance management requires using different techniques for different circumstances: sometimes directing traffic to different places is the right thing, sometimes bursting to the cloud, and sometimes knowing where traffic is emerging and building capacity before the traffic hits you.

At the same time, it is critical to build products and services in a sustainable way -- so that attacks on you do not result in long term harms, so that market changes don't leave you trapped, and so that regulators do not come to make your business plan impossible or destroy the value you have unlocked. By keeping an eye on the trends affecting Internet business, you can craft an Internet Performance Management strategy that makes your presence profitable and ensures your continued growth.

Specific knowledge of internet volatility, awareness of your options and the ability to affect rapid changes to internet paths is the province of Internet performance management. Employing proactive planning insights and quick, relevant problem analysis can make the Internet work for you rather than against. It's like the Corvair in a way. The original Corvair was a flawed and potentially dangerous vehicle. The original flaws in the car were in fact fixed by the time popular attention noticed the issues, but the bad publicity eroded sales. In the same way, you have the option to build your system right the first time. Internet performance management can be the way to get the design right, and to deliver what your customers want for a long time.

The future is here. Visit [dyn.com](https://dyn.com) to learn more.





# Rethink DNS.

Oracle Dyn is global business unit (GBU) focused on critical cloud infrastructure. Dyn is a pioneer in DNS and a leader in cloud-based infrastructure that connects users with digital content and experiences across a global internet. Dyn's solution is powered by a global network that drives 40 billion traffic optimization decisions daily for more than 3,500 enterprise customers, including preeminent digital brands such as Netflix, Twitter, LinkedIn and CNBC. Adding Dyn's best-in-class DNS and email services extend the Oracle cloud computing platform and provides enterprise customers with a one-stop shop for infrastructure as a service (IaaS) and platform as a service (PaaS).

Copyright © 2015, 2017, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. 1036

**ORACLE® + Dyn**

 [dyn.com](https://dyn.com)

 603 668 4998

 @dyn