UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of Technology

Remarks from the Office of Technology
By: Deputy Chief Technology Officer Alex Gaynor
At the FTC Panel Event on Cloud Computing: Taking Stock and Looking Ahead
Title: cloud-intro.docx

May 11, 2023

I'll start by saying these thoughts are my own, and don't necessarily represent the views of the Commission or any Commissioner.

As I was putting together these remarks, I realized I was coming up on 15 years of being a software engineer. Which means my career has roughly covered a timespan that started with the default being for a company to purchase its own servers, placed them in its own datacenters, and use them to run its own software. Now, many companies no longer own or operate any of their own physical servers, and instead they've migrated to cloud services, where they rely on a service provider to offer them virtual servers, and sometimes infrastructure that's even further abstracted from hardware.

A feature of my career having covered this transition is that I clearly remember the period in which I, and many peers and colleagues, hated the term "cloud". We thought it was vague, we thought it had no precise definition, and that meant it was destined to be a marketing buzzword, not something practitioners ever talked about. Like many changes in language, the word stuck, whether we liked it or not. But it still leaves us with the question of what exactly is a cloud?

It's common to organize cloud services into three high level buckets: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS products offer customers raw building blocks, such as servers, networking and storage. PaaS are more integrated offerings, which trade-off less flexibility with doing more out of the box. And finally, SaaS offerings are complete tools, rather than simply being building blocks. It's important to recognize that while these categories are useful, they are more of a spectrum than hard and fast distinctions. To further complicate matters, many cloud service providers have offerings from all of these categories at once.

These categories help us organize *within* cloud services, but they don't help us understand what a cloud is in the first place. For example, is a "private cloud", where developers create servers on demand, but the company still owns and runs physical infrastructure, really a cloud? It's a tough question, and the answer really depends on what's important to you about a cloud.
I'm a software engineer, so the best I can do is tell you what's been important to *me* about them. Rather than offering a formal market definition, I want to instead talk about three elements that help me distinguish cloud from non-cloud services:

> First, in the cloud, resources are elastic, it's possible to provision new servers and then spin them down at the snap of a finger. No longer are users reliant on placing orders for hardware and waiting for them to be delivered. For example, if you have a product that's more popular on the weekend than on weekdays, you can spin servers up Friday afternoon, and spin them down Monday morning.
>
> Second, you're billed by how much you use, not based on what you physically purchase. You can see how this is intimately linked to resource elasticity: if you use a server for 3 days or 3 minutes, you want to pay for that much usage. The utility of being able to spin up and down would be dramatically decreased without billing by usage.
>
> Finally, cloud services have APIs, which means you can write software to manage your infrastructure. To keep our example going, you might write a program that handles the scaling up on Fridays and down on Mondays, rather than doing it by hand each week.

Focusing on these elements, combined with the growth of PaaS and SaaS, are useful in understanding how, to an engineer, the cloud is different from what came before it.
There's no question that use of cloud infrastructure has become ubiquitous, and deeply intertwined with many of the other trends we see in technology: it's quite likely that any AI chatbots you've played with recently was running on a cloud.

Along with the clouds' ubiquity has come many security breaches which have cloud-specific features. For example, a fact pattern we've alleged in several cases is that one of the factors contributing to a company's poor security and data breaches is that they mismanaged and misconfigured their cloud systems. And while it's beyond question that companies have a responsibility to secure consumers' data effectively, whether in the cloud or not, it can also be instructive to ask: are there factors that make it more or less likely for cloud users to misconfigure their environments in the first place?

At the Commission's December Open Meeting, I spoke[1] about how the field of safety engineering teaches us that effective security programs don't accept "human error" as a final answer to why a vulnerability occurred, they use it as a jumping off point to ask deeper questions about how systems are designed. Because of their widespread use, when a cloud provider designs part of their system to be secure by default, all their customers benefit; but when a cloud provider designs its systems in a way that makes it easier to misconfigure something than they do to configure it securely, incidents can follow. Further, the set of offerings from some cloud providers are so expansive that knowing how to use them, and secure them, effectively is a challenge requiring dedicated expertise.

I'd be remiss if I didn't also take the time to share that I work for FTC's Office of Technology[2], created earlier this year. The role of our office is to build on the FTC's distinguished history of leveraging hands-on technical experts in its work. Events like these, with the goal of connecting

[1] https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/security-principles-addressing-underlying-causes-risk-complex-systems
[2] https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/02/century-technological-evolution-federal-trade-commission

the trends in technology with both our competition and consumer protection missions are central to what our office is here to do.

Thank you to the BCP, BC, OGC, OPP, and OT staff who reviewed and supported these remarks: Krisha Cerilli, Mark Eichorn, Peggy Bayer Femenella, Patricia Galvan, Hillary Greene, Ben Hendricks, Elisa Jillson, Nick Jones, Zehra Khan, Sam Levine, Steve Mohr, Kevin Moriarty, Joe Neely, John Newman, David Owyang, Stephanie Nguyen, Kelly Signs, Holly Vedova, James Weiss, and Ben Wiseman

***