STRINT Workshop Position Paper

20 January 2014
Larry Masinter, Adobe
Disclaimer: these personal opinions, not those of my employer.

I have three separate points:

1. "attack" is a bad metaphor

http://tools.ietf.org/html/draft-farrell-perpass-attack-03 is titled "Pervasive Monitoring is an Attack"
Calling pervasive monitoring an attack is misleading. Monitoring is trivially distinguishable from an "attack":

- There are multiple parties across the globe all engaged in various kinds of monitoring.
  An attack brings to mind a single attacker and a single defender.
- Much of the monitoring is passive; attack brings to mind an active injection of content or harm.
- An attack is generally focused in a limited period of time, while the surveillance of concern is ongoing and untargeted.
- An attack is intended as destructive specifically; surveillance is intended not to be noticed.

Metaphors matter:

http://www.w3.org/2001/tag/doc/governanceFramework-2012-07-19.html outlines three major problems with Internet governance.
Serious problems arise when regulation is written to the metaphors used to explain the technology. Calling monitoring an "attack" raises interest in responses that are not appropriate to the circumstances.

Don't. It's the wrong metaphor and the wrong rallying cry. It doesn't help explain the situation and can only backfire. Whatever the motivation, it seems likely the result will be the press picking up "attack" without reporting what was actually meant.

2. "Encryption Everywhere" is rarely helpful and sometimes harmful

This has been discussed at length, especially around proposals to encourage/enforce/keep HTTP/2 implementations & deployment encrypted. (See, e.g., William Chen). To recap:

- **Encryption everywhere can hurt privacy/security:**
  Whether it is, on average, a net improvement is debatable.
- **Encryption everywhere, even if it helps, doesn't help much**
  Private things are mainly already encrypted, and everything else has little information that isn't observable by knowing source, destination, timing, and payload size.
- **Encryption everywhere adds cost everywhere**:
  Exactly how much it costs and for whom is debatable, but it costs ***something*** in performance, complexity, computational power, bandwidth, latency.

3. Service concentration is a key factor in allowing pervasive monitoring

During most of the development of the Internet, the notion of planetary-scale computing would have been inconceivable: that it would be possible for a single organization to have sufficient capacity to offer some Internet service for everyone on the planet. But this has happened fairly recently. In consequence, scalability no longer limits monopoly. While competition is possible, economies of scale tip the balance toward a concentration of services. This is as intended—no one builds a planetary-scale service without hope of becoming a unique, proprietary platform. As designed, the systems inevitably devolve into a set where most traffic goes through a small number of service providers.

This is a problem for reliability and resilience as well as privacy: A small number of points of failure also are a small number of points of monitoring.

Too many Internet applications are being designed and deployed with a small number of service providers, for things like name lookup, identity, search, payment, instant messaging, file sharing. Further, applications and operating systems validate licenses, calling home, tracking usage. But if data is being gathered, it is also subject to monitoring.

We need to rethink the architecture of applications to reduce service bottlenecks. Is there a better design that makes pervasive monitoring more costly? Can we deploy more peer-to-peer and less client-server? The perspective I propose taking is looking more closely for these (mainly non-standard) points of monitoring, and work on how to distribute the previously concentrated work across the net to where pervasive monitoring is impractical, because a million sites would have to be monitored.