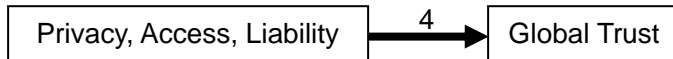# A Handy Internet Politics Measurement Note

Internet Politcs Measurement – Measurement and analysis on the Internet politics through case studies on (*i*) well-known but failed technical ideas in history, (*ii*) typical lawsuits related to the cyberspace, (*iii*) social problems related to the Intenet, etc.

Table of Contents

➢ **PKI**

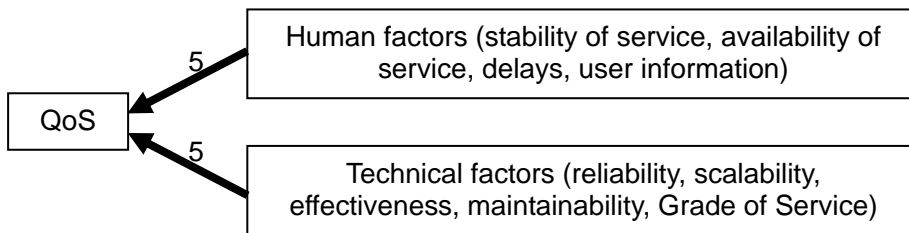| Privacy, Access, Liability | → 4 → | Global Trust |

The X.509 assumes a strict top-down hierarchical structure of trust which relies on a "self-signed" root that is trusted by everyone. The unreality of such a "self-signed" root impedes the X.509 from becoming a universal solution.

Vendors and entrepreneurs saw the possibility of a large market, started companies (or new projects at existing companies), and began to agitate for legal recognition and protection from liability. An American Bar Association technology project published an extensive analysis of some of the foreseeable legal aspects of PKI operations (see ABA digital signature guidelines), and shortly thereafter, several US states (Utah being the first in 1995) and other jurisdictions throughout the world, began to enact laws and adopt regulations. Consumer groups and others raised questions of privacy, access, and liability considerations which were more taken into consideration in some jurisdictions than in others.

PKI vendors have found a market, but it is not quite the market envisioned in the mid-90s, and it has grown both more slowly and in somewhat different ways than were anticipated. PKIs have not solved some of the problems they were expected to, and several major vendors have gone out of business or been acquired by others. PKI has had the most success in government implementations; the largest PKI implementation to date is the Defense Information Systems Agency (DISA) PKI infrastructure for the Common Access Cards program.

In comparison to Kerberos, PKI provides enhanced security, greater scalability and easier administration, control and management of the infrastructure. As a result, PKI enables a much larger community of users, consumers and partners to communicate and transact more dynamically, securely, reliably and cost-effectively.

➢ **QoS**

```
                    ┌──────────────────────────────────────┐
                    │ Human factors (stability of service, │
                    │ availability of                      │
              5     │ service, delays, user information)    │
┌──────────┐  ╱     └──────────────────────────────────────┘
│   QoS    │◄
└──────────┘  ╲  5  ┌──────────────────────────────────────┐
                    │ Technical factors (reliability,      │
                    │ scalability,                         │
                    │ effectiveness, maintainability,      │
                    │ Grade of Service)                    │
                    └──────────────────────────────────────┘
```

When the Internet was first deployed many years ago, it lacked the ability to provide Quality of Service guarantees due to limits in router computing power. It therefore ran at default QoS level, or "best effort". There were four "Type of Service" bits and three "Precedence" bits provided in each message, but they were ignored. These bits were later re-defined as DiffServ Code Points (DSCP) and are largely honored in peered links on the modern Internet.

When looking at packet-switched networks, Quality of service is affected by various factors, which can be divided into "human" and "technical" factors. Human factors include: stability of service, availability of service, delays, user information. Technical factors include: reliability, scalability, effectiveness, maintainability, Grade of Service, etc.
Many things can happen to packets as they travel from origin to destination, resulting in the following problems as seen from the point of view of the sender and receiver:

Dropped packets
The routers might fail to deliver (drop) some packets if they arrive when their buffers are already full. Some, none, or all of the packets might be dropped, depending on the state of the network, and it is impossible to determine what will happen in advance. The receiving application may ask for this information to be retransmitted, possibly causing severe delays in the overall transmission.

Delay
It might take a long time for a packet to reach its destination, because it gets held up in long queues, or takes a less direct route to avoid congestion. In some cases, excessive delay can render an application, such as VoIP or online gaming unusable.

Jitter
Packets from the source will reach the destination with different delays. A packet's delay varies with its position in the queues of the routers along the path between source and destination and this position can vary unpredictably. This variation in delay is known as jitter and can seriously affect the quality of streaming audio and/or video.
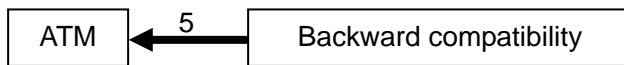
Out-of-order delivery
When a collection of related packets is routed through the Internet, different packets may take different routes, each resulting in a different delay. The result is that the packets arrive in a different order than they were sent. This problem requires special additional protocols responsible for rearranging out-of-order packets to an isochronous state once they reach their destination. This is especially important for video and VoIP streams where quality is dramatically affected by both latency and lack of isochronicity.
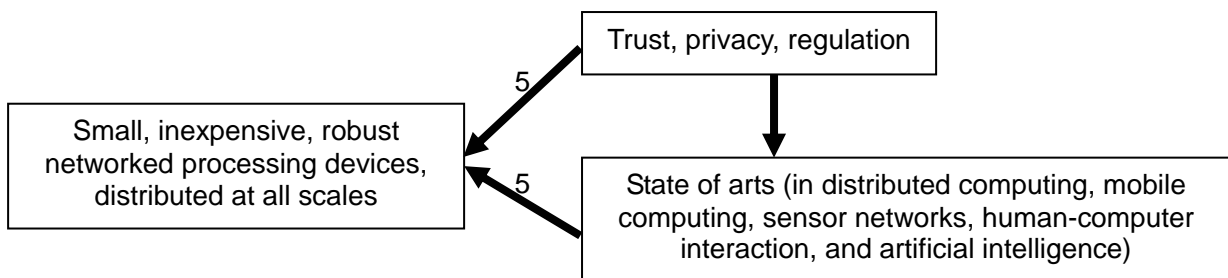
Error
Sometimes packets are misdirected, or combined together, or corrupted, while en route. The receiver has to detect this and, just as if the packet was dropped, ask the sender to repeat itself.

> **ATM**

```
┌─────────┐       5      ┌────────────────────────┐
│   ATM   │ ◄───────────│  Backward compatibility │
└─────────┘              └────────────────────────┘
```

ATM has proven very successful in the WAN scenario and numerous telecommunication providers have implemented ATM in their wide-area network cores. Many ADSL implementations also use ATM. However, ATM has failed to gain wide use as a LAN technology, and its complexity has held back its full deployment as the single integrating network technology in the way that its inventors originally intended. Since there will always be both brand-new and obsolescent link-layer technologies, particularly in the LAN area, not all of them will fit neatly into the synchronous optical networking model for which ATM was designed. Therefore, a protocol is needed to provide a unifying layer over both ATM and non-ATM link layers, as ATM itself cannot fill that role. IP already does that; therefore, there is often no point in implementing ATM at the network layer.

> **Ubiqutous Computing**

```
                              ┌──────────────────────────┐
                              │  Trust, privacy, regulation │
                              └──────────────────────────┘
            5 ↙                            │
┌────────────────────────┐                 ▼
│  Small, inexpensive, robust │    ┌────────────────────────────────────┐
│  networked processing devices, │  │ State of arts (in distributed computing, mobile │
│    distributed at all scales │ ◄─│ computing, sensor networks, human-computer │
└────────────────────────┘  5   │   interaction, and artificial intelligence) │
                                 └────────────────────────────────────┘
```

Mark Weiser coined the phrase "ubiquitous computing" around 1988, during his tenure as Chief Technologist of the Xerox Palo Alto Research Center (PARC).
Ubiquitous computing is a post-desktop model of human-computer interaction in which information processing has been thoroughly integrated into everyday objects and activities. As opposed to the desktop paradigm, in which a single user consciously engages a single device for a specialized purpose, someone "using" ubiquitous computing engages many computational devices and systems simultaneously, in the course of ordinary activities, and may not necessarily even be aware that they are doing so.

At their core, all models of ubiquitous computing share a vision of small, inexpensive, robust networked processing devices, distributed at all scales throughout everyday life and generally turned to distinctly quotidian ends. For example, a domestic ubiquitous computing environment might interconnect lighting and environmental controls with personal biometric monitors woven into clothing so that illumination and heating conditions in a room might be modulated, continuously and imperceptibly. Another common scenario posits refrigerators "aware" of their suitably-tagged contents, able to both plan a variety of menus from the food actually on hand, and warn users of stale or spoiled food.

Contemporary human-computer interaction models, whether command-line, menu-driven, or GUI-based, are inappropriate and inadequate to the ubiquitous case. This suggests that the "natural" interaction paradigm appropriate to a fully robust ubiquitous computing has yet to emerge - although there is also recognition in the field that in many ways we are already living in an ubicomp world. Contemporary devices that lend some support to this latter idea include

mobile phones, digital audio players, radio-frequency identification tags and interactive whiteboards.

Ubiquitous computing encompasses a wide range of research topics, including distributed computing, mobile computing, sensor networks, human-computer interaction, and artificial intelligence.

> **Bankruptcy of Napster**

| Creativity | ←— 4 — | Copyright |
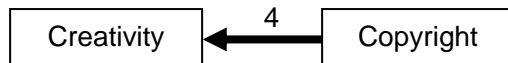
In 2000, A&M records and several other recording companies sued Napster (A&M Records, Inc. v. Napster, Inc.) for contributory and vicarious copyright infringement under the US Digital Millennium Copyright Act (DMC Act).[6] The music industry made the following claims against Napster : (1) That its users were directly infringing the plaintiff's copyright; (2) That Napster was liable for contributory infringement of the plaintiff's copyright; and (3) That Napster was liable for vicarious infringement of the plaintiff's copyright.

The court found Napster guilty on all three claims.

Napster lost the case in the District Court and appealed to the U.S. Court of Appeals for the Ninth Circuit. Although the Ninth Circuit found that Napster was capable of commercially significant non-infringing uses, it affirmed the District Court's decision. On remand, the District Court ordered Napster to monitor the activities of its network and to block access to infringing material when notified of that material's location. Napster was unable to do this, and so shut down its service in July 2001. Napster finally declared itself bankrupt in 2002 and sold its assets. It had already been offline since the previous year owing to the effect of the court rulings.

> **Abuse of Censorship-free Speech, "Human Search Engine" (China)**

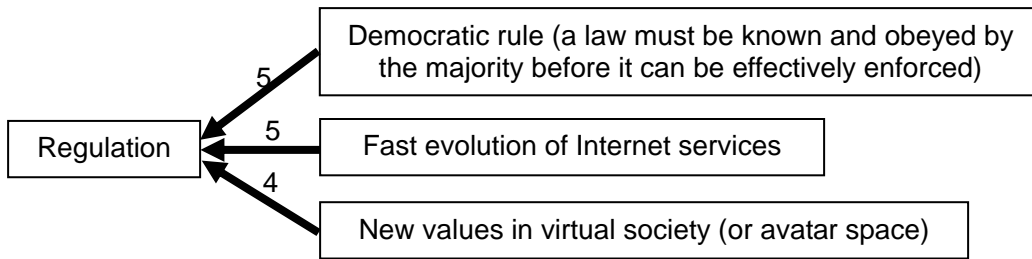| Regulation | ←— 4 — | Censorship-free speech |
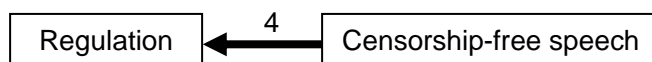
Human search engine – Use common efforts of Internet users to manually find out a person's real identity.

When a person did something wrong which incured public disagreement and condemnation, some people unduely exploited the human search engine to find her real identity. As a result, private information (e.g., real name, address, phone no, school) of this person is exposed to the public. Her family are therefore harassed and threatened by extremists.

The above situation is an "Internet volience" issue that caused more and more public concerns in China in the last two years.

> **Difficulty to Enforce Cyberlaws and Related Regulations (Japan, Germany, US)**

```
                    ┌─────────────────────────────────────────────┐
              5     │ Democratic rule (a law must be known and obeyed by │
            ┌───────│   the majority before it can be effectively enforced) │
┌──────────┐│   5   └─────────────────────────────────────────────┘
│ Regulation │◄──────┌─────────────────────────────────────┐
└──────────┘│   4   │    Fast evolution of Internet services     │
            └───────└─────────────────────────────────────┘
                    ┌─────────────────────────────────────────────┐
                    │   New values in virtual society (or avatar space) │
                    └─────────────────────────────────────────────┘
```

Although there are very rigid and accurate cyberlaws and regulations having been enacted in Japan and Germany, annoucement and propagation speed of these laws and regulations are unable to keep up with the necessary pace, therefore the law enforecment efficacy is very limited.

The following story is about a lawsuit for a case happened in the avartar space. It is cited from the book *CODE* (version 2) by lawrence lessig:

The argument was about borders—about where her land stopped. It seemed like a simple idea, one you would have thought the powers-that-be would have worked out many years before. But here they were, her neighbor Dank and she, still fighting about borders. Or rather, about something fuzzy at the borders—about something of Martha's that spilled over into the land of others. This was the fight, and it all related to what Martha did.

Martha grew flowers. Not just any flowers, but flowers with an odd sort of power. They were beautiful flowers, and their scent entranced. But, however beautiful, these flowers were also poisonous. This was Martha's weird idea: to make flowers of extraordinary beauty which, if touched, would kill. Strange no doubt, but no one said that Martha wasn't strange. She was unusual, as was this neighborhood. But sadly, disputes like this were not.

The start of the argument was predictable enough. Martha's neighbor, Dank, had a dog. Dank's dog died. The dog died because it had eaten a petal from one of Martha's flowers. A beautiful petal, and now a dead dog. Dank had his own ideas about these flowers, and about this neighbor, and he expressed those ideas—perhaps with a bit too much anger, or perhaps with anger appropriate to the situation.

"There is no reason to grow deadly flowers," Dank yelled across the fence. "There's no reason to get so upset about a few dead dogs," Martha replied. "A dog can always be replaced. And anyway, why have a dog that suffers when dying? Get yourself a pain-free-death dog, and my petals will cause no harm."

...

The best example of this space today is the extraordinary community of Second Life. In it, people create both things and community, the avatars are amazingly well crafted, and their owners spend hundreds of thousands of hours building things in this space that others see, and some enjoy. Some make clothes or hair styles, some make machines that make music. Whatever object or service the programming language allows, creators in Second Life are creating it. There are more than 100,000 residents of Second Life at the time of this writing. They occupy close to 2,000 servers housed in downtown San Francisco, and suck 250 kilowatts of electricity just to run the computers—about the equivalent of 160 homes.

But here we get back to Martha and Dank. In their exchange—when Martha blamed Dank for having a dog that died with pain—they revealed what was most amazing about that particular

MMOG. Martha's remarks ("Why do you have a dog that suffers when dying? Get yourself a pain-free-death dog, and my petals will cause no harm") should have struck you as odd. You may have thought, "How weird that someone would think that the fault lay not in the poisonous petals but in a dog that died with pain." But in this space, Dank did have a choice about how his dog would die. Maybe not a choice about whether "poison" would "kill" a dog, but a choice about whether the dog would "suffer" when it "died." He also had a choice about whether a copy of the dog could be made, so that if it died it could be "revived." In MMOG space, these possibilities are not given by God. Or rather, if they are defined by God, then the players share the power of God. For the possibilities in MMOG space are determined by the code—the software, or architecture, that makes the MMOG space what it is. "What happens when" is a statement of logic; it asserts a relationship that is manifested in code. In real space we don't have much control over that code. In MMOG space we do.

➢ **Internet Addiction, "Impact on Minority" (e.g. online ponography for children)**
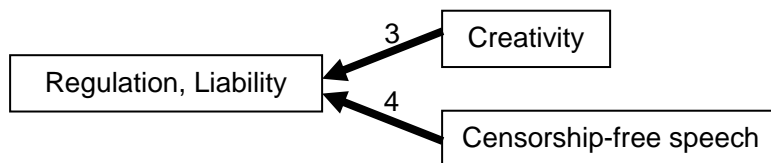
According to [4], more than one out of eight Americans exhibits signs of Internet addiction. The biggest culprit of Internet addiction is not online pornography, games and gambling as some people think, but ordinary services such as email, online chatting and shopping.

[4] E. Aboujaoude, L. Koran, N. Gamel, M. Large, and R. Serpe. Potential markers for problematic Internet use: a telephone survey of 2,513 adults. CNS Spectrums: The International Journal of Neuropsychiatric Medicine, 2006.

Collective violence cases (including sexual violence) frequently happened in primary schools of Korea in 2008.

➢ **Frustration of eBay, Yahoo, Amazon and Google in China**
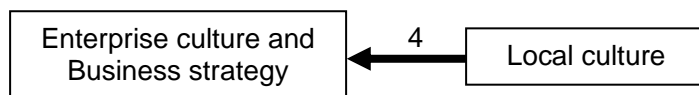
eBay was beaten by TaoBao (taobao.com)
Yahoo and Google was beaten by Baidu (baidu.com)
Amazon was beaten by AliBaBa (alibaba.com)
MSN was beaten by QQ

Several contrasts:

   "Favor the 'white-collars' at the cost of losing the average public"
      vs.
   "Meet with interest of the public majority"

   "Prevent from being hated by the public even if at the cost of being forgotten by the public"
      vs.
   "Prevent from being forgotten by the public even if at the cost of being hated by the public"

"Focus on long-term business strategy"
    vs.
"Focus on short-term business tactics"
→ Although those large multinational Corporations have a strategic ten-year-loss plan, they usually were unable to turn the trend of loss after the ten years.

"Advertisement and promotion via email, phone, MSN"
    vs.
"Advertisement and promotion in person (face-to-face)"

> **Internet Politics Measurement Papers or Internet Politics Forum ?**
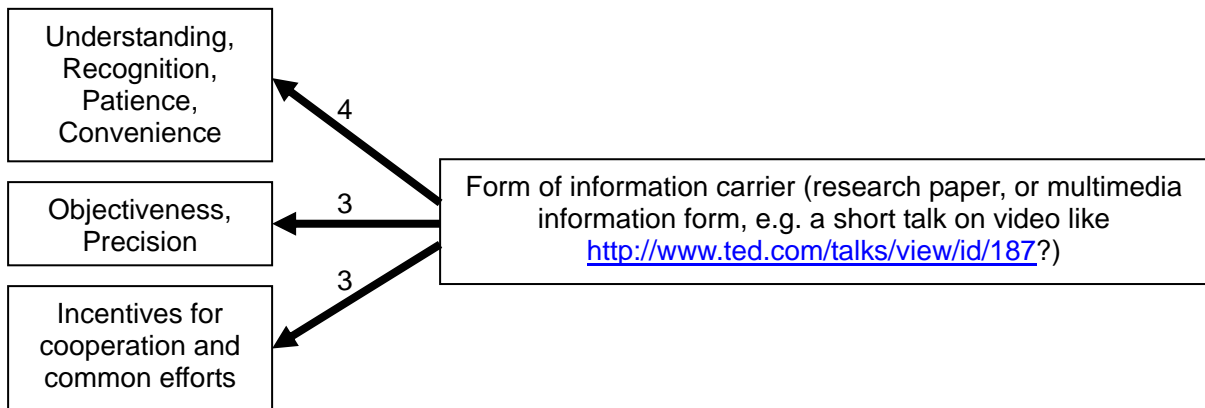
Which way might be more suitable to derive an objective view of the Internet politics from subjective views of individuals?

Having people publish papers about "Internet politics measurement"?
    or
Having people engage in the "Internet politics forum"?