Digital Revolution, Free Software and the Normative Process

Prof. Pedro A. D. Rezende

Computer Science – University of Brasília

pedro.jmrezende.com.br/sd.php

Revolution ou Evolution?

Evolution of digital computing

Decade	Innovation	Paradigm (challenge): How can there be ...	Dominant D&L Model
1940	Architectures	Programmable computers?	Hardware <-> Software
1950	Transistors	Viable programs?	
1960	Source code	Useful viability?	Hw +Sw +Service Level Agreement
1970	Algorithms	Efficient usefulness?	
1980	Downsize+nets	Productive efficiency?	SW = End User License Agreemnt
1990	Internet	Trustful productivity?	
2000	Ciberculture	Virtualizable trust?	? FOSS ? SaaS ?

Digital Revolution

Decade	Innovation	Paradigm (challenge): How can there be ...	Dominant D&L Model
1940	Architectures	Programmable computers?	**Craftsmanship:** Hw <-> Sw
1950	Transistors	Viable programs?	
1960	Source code	Useful viability?	**Monolithic:** Hw + Sw + SLA
1970	Algorithms	Efficient usefulness?	
1980	Downsize+nets	Productive efficiency?	**Proprietary:** Sw = EULA
1990	Internet	Trustful productivity?	
2000	Ciberculture	Virtualizable trust?	**?**

P-M

M-M

P-P

Socio-technical transitions related to the emergence of new *forms* of communication

Socio-technical Transitions

- Through socio-technical transitions, the digital revolution changes power relations, in favor of those who control the new informational flows.

- In information societies, where social practices are increasingly intermediated by Information and Communication Technologies (ICT), the control of the new informational flows is achieved not only by technical know-how, but also, by dominating the normative process that regulates the use of ICT.

Normative Process

- Normative domination is achieved, in various dosages, by controlling the setup and deployment of ICT (Lawrence Lessig: *Code is law*), and by steering the legislative processes to enforce ICT usage under such controls, or to forbid usage beyond them.

- This juncture transforms the political theater, wherein the roles and strategic actions by the State and by large corporations suffer profound changes.

- Changes mainly induced by shifts provoked by this usage, for the various interests involved, in the frontier of optimum efficiency between *competition* and *cooperation*.

Critical Juncture

- A limited perception of this juncture, and of what is at stake in its possible unfoldings, can produce distopias, such as the illusion that FOSS is “anti-business”, or that the current economic crisis signals exhaustion of neoliberal ideology and economic models.

- We offer an analysis of this juncture according to which the current crisis, *on the contrary*, represents new opportunities for unilateralist offensives. In these offensives, hegemonic and monopolist interests cooperate, through the normative control of TICs, to achieve their goals “in the name of the public interest”. (see Naomi Klein: “*The Shock Doctrine*”)

Axis of analysis

- The axis of analysis will be on recent initiatives taken by nations which are central to capitalism, aimed at negotiating global treaties to combat new modalities of crimes. These initiatives are allegedly justified by a supposed “lack of norms and laws” arisen from the dissemination of TIC usage (i.e., cybercrime). We look at the *Broadcast Treaty*; Budapest Convention, and ACTA.

- Brazil did not and does not take part in the negotiations of the last two. Nevertheless, it receives great diplomatic pressure to adhere to the first, against its established policy of not adhering to international treaties in which negotiations it did not participate.

Game plan

- What these treaties reflect is a search for efficacy in combating various conducts already typified as crime, but practiced with the use of TIC. But, what these treaties *obfuscate* is the economic logic which calibrates the definition of new crimes, the methods of enforcement, and the possible / probable collateral effects from the interaction between these new definitions and methods.

- In perspective, what these negotiations reveal is a strategy for a progressive enclosure, leading to a normative besieging of cyberspace, a kind of *virtual ratcheting* of symbolic goods and informational flows. This begs the question of whose interest outside the negotiation processes will be met or prejudiced.

Normative enclosure strategies

Forum shifting: TRIPS(+), Broadcast, Budapest, towards ACTA.

Secret negotiations towards ACTA leak slowly.

Intellectual property "bridges": At least one has been crossed

Lawsuit MS vs. TomTom: frivolous patents against Linux (FAT)

Legal Uncertainty (Software patents)

Testing the abuse limits: US Supreme Court In **Re Bilski** case:

Legal insecurity: Technical effect or transformative effect?

Conections

How do these strategies converge to a "ratcheted enclosure"?

1st strategy: *Forum shifting*

- Monopolist interests in the TIC area tend to embrace a normative strategy for proprietarization of knowledge. To monetize it, they have to induce artificial scarcity (of symbolic goods). Thus, they have to promote the radicalization of IP laws ('strong IP'). They do so in many initiatives: WTO (TRIPS), WIPO (SCCR), EU, ALCA

- When an initiative is neutralized by organized cooperation in the periphery of capitalism, they put it in standby and regroup, founding or capturing another stance, forum or negotiating agenda

- Shifts between 2007 and 2009: OMPI -> TRIPS+ (Patents)
 OMPI -> EU (Broadcast treaty); OMPI -> ACTA (“PI” + etc.);

Towards an Anti-Counterfeiting Trade Agreement (ACTA)

2004 – The original agenda (was very different than today's)**:**
tracs.co.nz/gripping-hand/charge-of-the-ip-brigade

Oct 07- USA, European Union, Japan, S. Korea, Mexico, N. Zealand, Switzerland and Canada announced plans to negotiate an "anti-counterfeiting" treaty
www.michaelgeist.ca/content/view/3786/125

Until Apr 08 - Some of these countries (such as Canada) sought internal support for the initiative, others did not (such as USA). About the matter under negotiation, only the chapter titles of the would-be treaty were revealed:

Towards ACTA

Until Apr 08 – Chapters of the proposal being negotiated:

(1) Initial Provisions and Definitions;

(2) Enforcement of Intellectual Property Rights;

(3) International Cooperation;

(4) Enforcement Practices;

(5) Institutional Arrangements;

(6) Final Provisions.

Throughout 2008 some documents leaked to wikileak (negotiators neither confirm nor deny their authenticity)

Towards ACTA

3-4 jun 08 – First Round of secret negotiations, chaired by the US Trade Representative at US mission in Geneva, with delegations from Australia, Canada, European Union Presidency (Slovenia), Japan, S. Korea, Mexico, Morocco, New Zealand, U. Arab Emirates, USA.

"Non-papers" (balões de ensaio) were circulated on institutional arrangements and enforcement; US and Japan offered a draft on enforcement of IPR containing measures such as:

1- *Customs officers would be able to block shipments on their own initiative, supported by information supplied by rights holders*.

Towards ACTA

3-4 Jun 08 - (continuation) Draft for Enforcement of IPR:

2- *Those same custom officers would have the power to levy penalties if the goods are infringing*.

3- *US would like a provision that absolves rights holders of any financial liability for storage or destruction of the infringing goods.*

4- *Also, that the officers which have detained infringing goods, shall inform the right holder of the names and addresses of the consignor, importer, exporter, or consignee, and provide to the right holder a description of the goods and of the transaction yielding its transportation.*

Towards ACTA

29-31 Jul 08 - Second round, in Washington DC, USA with Singapura joining in, U. Arab Emirates drooping out. Laconic press release, with nothing substantial on the negotiations per se.

Discussions focussed on border measures (second time), civil enforcement (first time), as well as non-papers on institutional issues and international cooperation.

USA and Japan again asked for civil enforcement provisions against would be violators of any imaterial property rights, including patents (which include, of course, *software patents*), cultivar seeds, copyrights and trademarks.

Towards ACTA

29-31 Jul 08 - (continuation) Second round:

- Parties to the treaty would be required to implement procedures that include the availability of statutory damages for copyright and trademark infringement (some countries would like this to be optional, while the U.S. would like the damages provisions expanded to patent infringement) as well as court costs.

This statutory damages provision includes:

Towards ACTA

29-31 Jul 08 - (continuation) Provision drafted:

1. *Each Party shall provide that in civil judicial proceedings, its judicial authorities on application of the injured party shall have the authority to order the infringer who knowingly or with* ***reasonable grounds to know****, engaged in infringing activity of intellectual property rights to pay the right holder damages adequate to compensate for the actual prejudice the right holder has suffered as a result of the infringement, taking into account all appropriate aspects, inter alia, the* ***lost profits****, the value of the infringed good or service, measured by the market price, the suggested retail price, unfair profits and* ***elements other than economic factors*** *or* ***other legitimate measure of value*** *submitted by the right holder.*

Towards ACTA

8-9 Oct 08- Third round, in Toquio, Japan.
Again, only a laconic press release.

The U.S. and Japan supply draft text of the criminal enforcement provisions. The proposal would extend criminal enforcement to both (1) cases of a commercial nature; and (2) cases involving significant willful copyright and trademark infringement even where there is no direct or indirect motivation of financial gain. The treaty would require each country to establish a laundry list of penalties - including imprisonment - **sufficient to deter future acts of infringement**.

Specifically:

Towards ACTA

8-9 Oct 08 - (continuation) Criminal enforcement provision: *Each Party shall provide that in civil judicial proceedings concerning the enforcement of intellectual property rights, its judicial authorities* ***shall have the authority to order the infringer to provide****,* ***for the purpose of collecting evidence****,* ***any information that the infringer*** *possesses or* ***controls****, to the right holder or to the judicial authorities. Such information may include information regarding any person or persons involved in any aspect of the infringement and regarding the means of production or distribution channel of such goods or services, including* ***the identification of third persons involved in the production and distribution of the infringing goods or services or in their channels of distribution****.*

Towards ACTA

8-9 Oct 08 - (continuation) Criminal enforcement provision: *"... include sentences of imprisonment as well as monetary fines sufficiently high to provide a deterrent to future acts of infringement, consistent with a policy of removing the monetary incentive of the infringer .... Each Party shall provide for **criminal procedures** and penalties to be applied, **even absent willful** trademark counterfeiting or copyright or **related rights piracy**, at least in cases of knowing trafficking in: (a) counterfeit labels affixed to, enclosing, or designed to be affixed to, enclose, or accompany: (i) a phonogram, (ii) a copy of a **computer program** or other literary work, (iv) documentation or packaging for such items; and (b) counterfeit documentation or package for items of the type in (a); and (c) illicit labels affixed to..."*

Towards ACTA

15-18 Dec 08 - Forth round, in Paris, France.
Again, only a laconic press release.

Institutional Arrangements and negotiation on criminal enforcement (first raised in Tokyo) were discussed. The U.S. provides a "non-paper" on the Internet, and probes each delegation to answer questions on the state of their domestic law. The paper discusses Internet copyright provisions, liability for Internet service providers, and legal protection for digital locks (DRM). The probe raises questions about damage awards, liability for hosting or storing content, and the extent to which the anti-circumvention provisions mirror the USA approach to **virtual ratcheting**:

Towards ACTA

15-18 Dec 08 - (continuation) Probing questions:

The probe raises questions about damage awards, liability for hosting or storing content, and how far local anti-circumvention provisions (DRM-as-law) mirror USA's approach to **virtual ratcheting**:

Towards ACTA

Feb 09 - USA asks ACTA negotiating partners for the postponement of the fifth round, scheduled for March, in order to give time to President Obama to pick his USTR staff.

Mar 09 – The European Parliament approves a resolution demanding that EU ACTA negotiators release any and all material produced for or during the negotiations to interested parties (so far disobeyed)

At the same time, USA government denies similar request, filed under FOIA (Freedom of Information Act) rules, alleging "*homeland security*" reasons.

pjustice.org/wp/campaigns/acta

keionline.org/acta-petition

Towards ACTA

12 Jun 09 - Australia, Canada, European Union, Japan, S Korea, Mexico, Morroco, N. Zealand, Singapure, Switzerland, USA issue a joint press release announcing they are *“moving forward”* in negotiations towards an *Anti-Counterfeiting Trade Agreement* “*to advance the global fight against* counterfeiting **and piracy**”

? - 17 Jul 2009 - Fifth round, in Morroco,
No press release, no leaks.

Nov 2009 - Sixth round, scheduled for S. Korea**,**
Aiming to reach a Treaty Agreement by 2010.
www.international.gc.ca/trade-agreements-accords-commerciaux/fo/press-release-communique.aspx

2nd strategy: *“IP Bridges”*

Semi-secret agreements between monopolists and companies developing or making money with free software, with the goal of "protecting" both and their clients against legal threats via patent ambushes, but also effective against other free software developers and corporate clients (weakening the collaborative development process and threatening FOSS user rights).

- Those involved call these agreements “IP bridges”
- The technical camouflage for these business weapons is interoperability (selective interoperability = *vendor lock-in*).

Example.: Microsoft – Novell, 2007

Where do “IP bridges” take us?

To Cyberracketing

(Virtual racketing to besiege cyberspace)

Example 1: (US Federal Circuit Nº 07-1545)

Patent ambush in standard H.264 (MPEG 2 and MPEG 4 *upgrades*)

Qualcomm vs. Broadcom (appeal, Sep 2008)

iplawobserver.com/2008/12/qualcomm-penalized-for-failure-to.html

Example 2: (Adobe, ODF Alliance vs. Microsoft)

Guerrilla tactics (*Embrace, Extend, Extinguish*) against open standards for electronic document formats (pdf, ODF) www.robweir.com/blog/ june.9.09; news.cnet.com/2100-1012_3-6079320.html

Example 3: (US District Court Washington , ITC, 26 fev 2009)

Frivolous patents upheld by USPTO 5579517, 5758352, 6256642

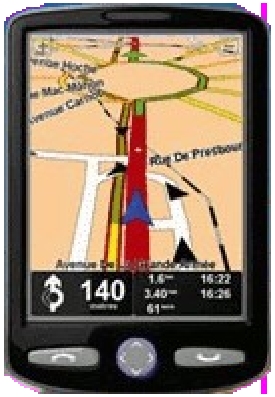
(File Allocation Table naming) to be used in extortion attacks against Linux arstechnica.com/old/content/2006/01/5959.ars Microsoft vs. TomTom.

Cyberracketing

Example 3:

TomTom is a main supplyer of graphical GPS mapping devices and services.

It was the main supplyer under a GNU/Linux platform



Although it faught back (in Mar 20, 09), and joined the Open Innovation Network (OIN) in Mar 23, 09, the company was bkackmailed and coopted to the Windows Mobile platform, after a secret agreement that settled the lawsuit (Mar 30, 09)
www.tomtom.com/products/category.php?ID=2
itmanagement.earthweb.com/osrc/article.php/12068_3807801_3/

TomTom's main competitor, Garmin, uses the Windows Mobile platform.
reuters.com/article/companyNewsAndPR/idUSLQ40872620090226

Cyberracketing

Example 3:

With TomTom blackmailed and coopted to the Windows Mobile platform, now all the main suplliers of graphical GPS mapping devices and services use it. itmanagement.earthweb.com/osrc/article.php/12068_3807801_3. Then ...

Cyberracketing

Example 3:

With TomTom blackmailed and coopted to the Windows Mobile platform, now all the main suplliers of graphical GPS mapping devices and services use it. itmanagement.earthweb.com/osrc/article.php/12068_3807801_3. Then ...

Provision in EULA for Web Viewer (Windows Mobile's browser):

> “*The Software may contain third party software which requires notices and/or additional terms and conditions. Such required third party software notices and/or additional terms and conditions are made a part of and incorporated by reference into this EULA. By accepting this EULA, you are also accepting the additional terms and conditions, if any, set forth therein.*”

www.boingboing.net/2007/10/11/crazy-eula-makes-you.html

Cyberrracketing via “MS tax”

Exampe 4:

Dana Blankenhorn looked for penguins in Taiwan's Computex 2009 (June 2): “*It was depressing. It’s not just Asus and MSI who have gone Windows in Taiwan, it’s everyone*”

Why?

Cyberrracketing via “MS tax”

Exampe 4:

Dana Blankenhorn looked for penguins in Taiwan's Computex 2009 (June 2): *“It was depressing. It’s not just Asus and MSI who have gone Windows in Taiwan, it’s everyone*”

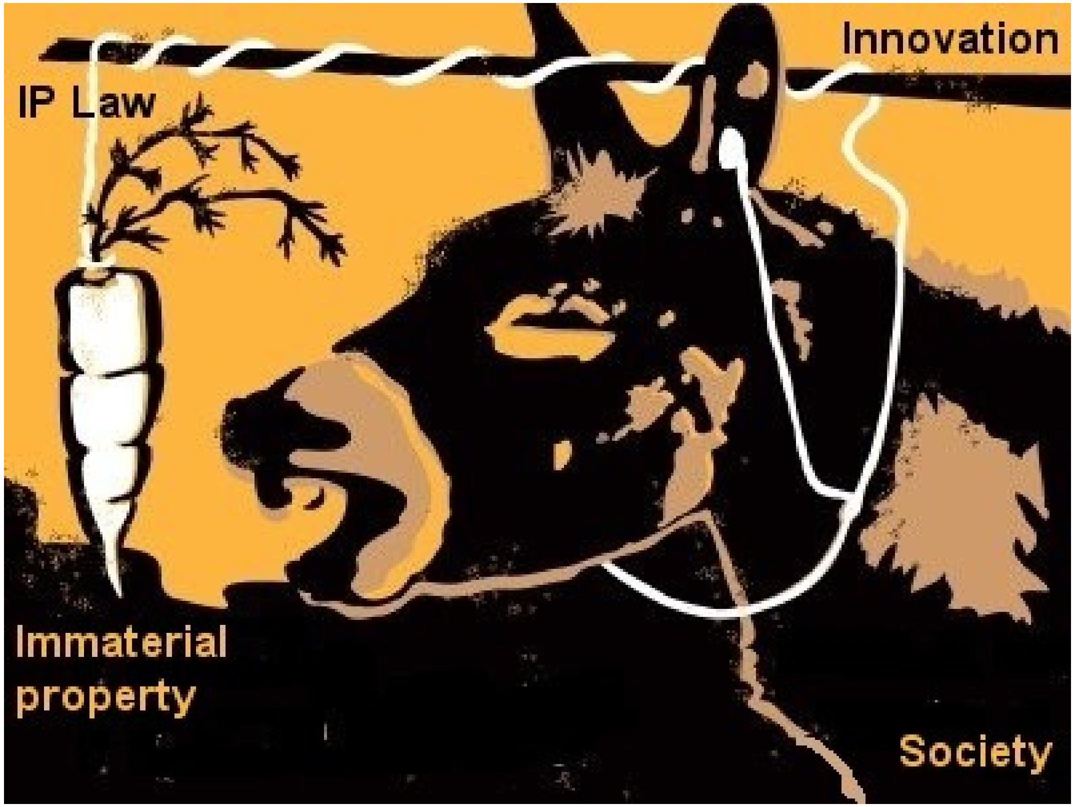
Why?

The Vice President of Taipei Computer Association Responds: *“In our association we operate as a consortium, like the open source consortium. They want to promote open source and Linux. But if you begin from the PC you are afraid of Microsoft. They try to go to the smart phone or PDA to start again.*”

blogs.zdnet.com/open-source/?p=4311#more-4311

Who crosses the “IP bridge”?

? ←



The cyber-racketed, victims of the Digital Stockohlm Syndrome

3rd strategy: *Legal uncertainty*

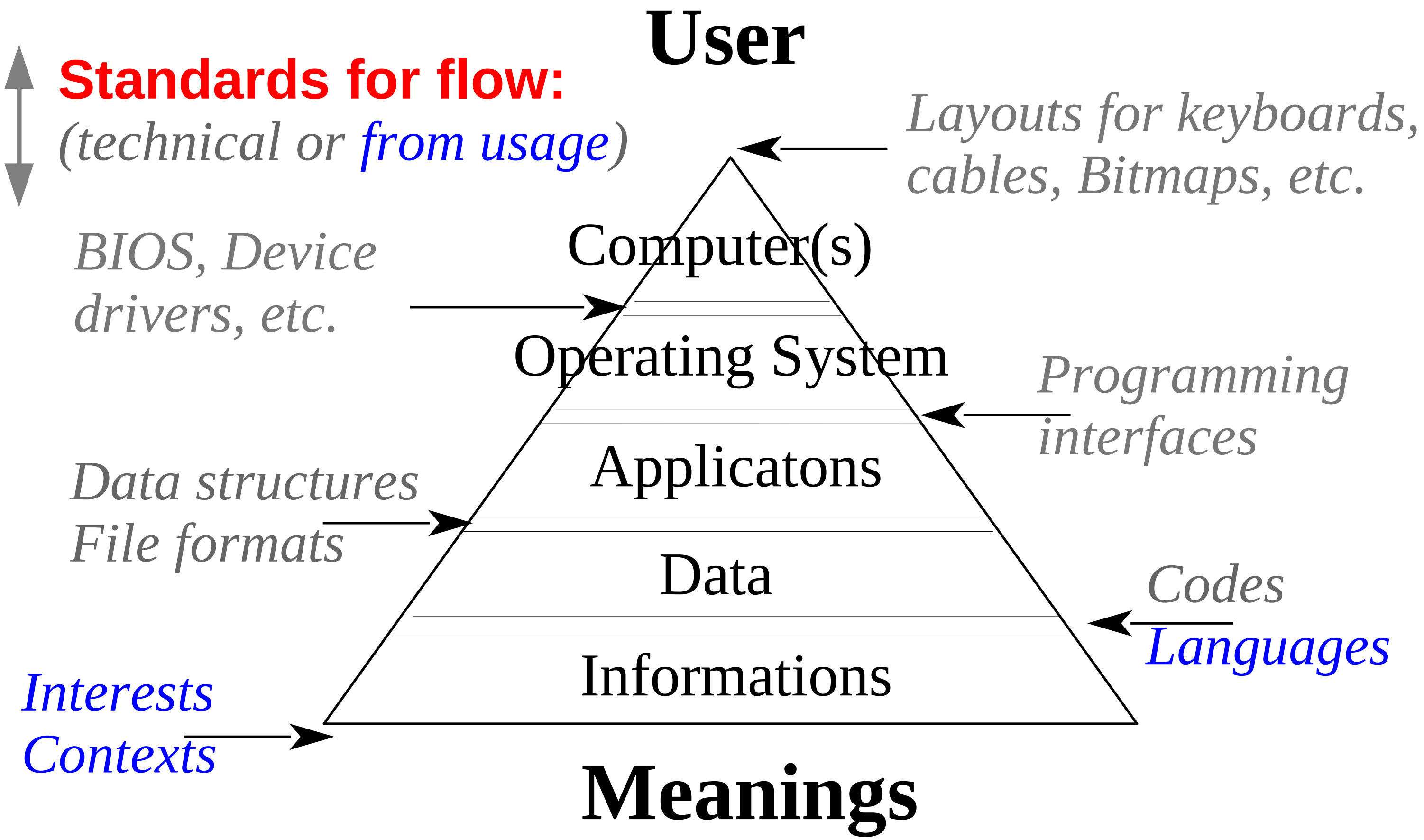
Re Bilski in the US Supreme Court:

After decades ignoring it, the US Supreme Court will hear a case pertaining to the patenteability of ideas implemented by software: Bilski wanted to patent a method for leveraging risk against losses with commodities due to weather conditions, for use in the stock market.
- He was denied a patent by the USPTO, he appealed to CAFC and lost.

The US Supreme Court wants to decide by setting a distinction between:

Software "as such" (does **not** produce "technical" or "transformative" effect) [example: "mathematical algorithm"] versus
Software "beyond such" (does produce "technical" or "transformative" effect) [example: "**non**-mathematical algorithm"]

What is Informatics?



User

Standards for flow:
(technical or from usage)

Layouts for keyboards, cables, Bitmaps, etc.

Computer(s)

BIOS, Device drivers, etc.

Operating System

Programming interfaces

Applicatons

Data structures
File formats

Data

Codes
Languages

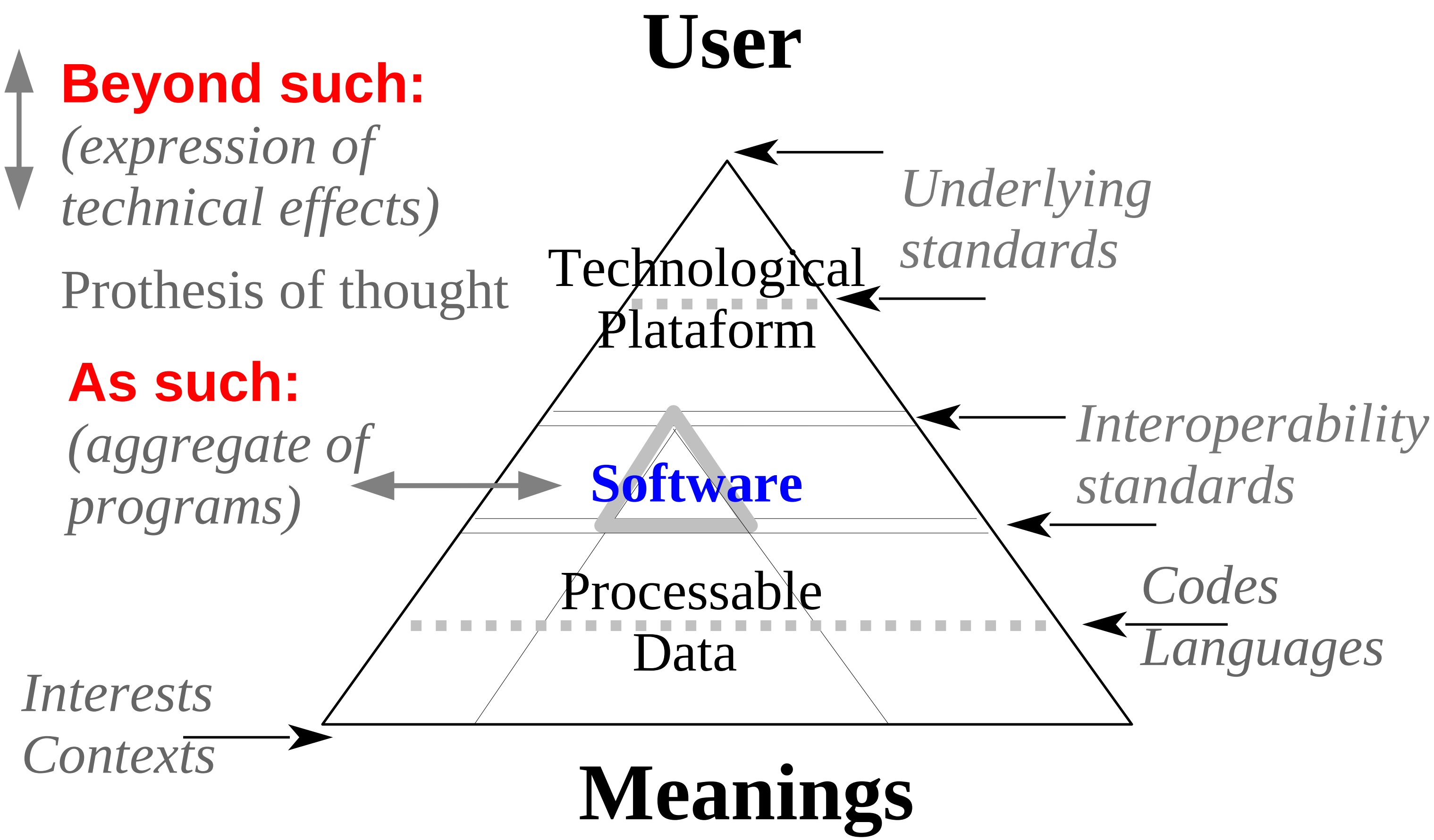
Informations

Interests
Contexts

Meanings

Prodution of meaning intermediated by TIC

What is Software?



User

Beyond such:
(expression of technical effects)

Prothesis of thought

As such:
(aggregate of programs)

Technological Plataform

Software

Processable Data

Underlying standards

Interoperability standards

Codes
Languages

Interests
Contexts

Meanings

Prodution of meaning intermediated by computer programs

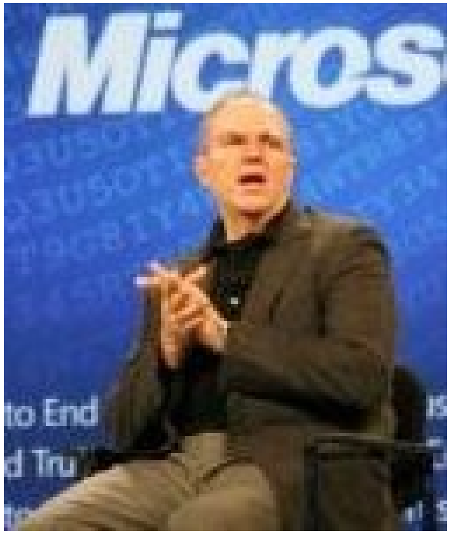
Conections

Abr 09 – Phillip Hallam-Baker, at MIT Ciber International Relations Conference

> *"The information we have on opposition activities is highly unsatisfactory. By the time an Internet crime trend can be reliably quantified it is obsolete. And even though we have no shortage of technical countermeasures, we have only succeeded in deploying measures that provide a short term tactical benefit to the deploying party rather than strategic measures that could defeat or at the very least dramatically raise the bar for the opposition."* csail.mit.edu/events/eventcalendar/calendar.php?show=event&id=2188

Conections

Abr 08 - Craig Mundie
at RSA Conference '08



*"The **foundation** has been laid for good security practices. The **challenge** now is related to **management practices** ... The overall management systems today are not **integrated** enough, they're too complicated. That has been a **major focus** for Microsoft."*

MS Trusted Computing Group Manager:

*"With everything we do, there's always skepticism and conspiracy theories. The answer is no; **this is for real**."*

www.news.com/8301-10784_3-9914240-7.html?tag=yt

This *is* for real

Jun 08 Craig Mundie

- Substituted Bill Gates as CEO at MS

- Participantes in Bilderberg Group

(together with Google's Eric Schmidtt, etc.)

Bilderberg Group

A closed social club, with 200 of the richest and most powerful businessman and bankers in the planet? A global secret proto-government? Some of both?

infowars.com/articles/nwo/bilderberg_07_welcome_to_lunatic_fringe.htm

en.wikipedia.org/wiki/List_of_Bilderberg_attendees

This *is* for real

Moral Hazzard, in the US: *Shoplifting costs retail businesses $35+ million per day, as 27 million shoplifters go on the hunt. Insurance fraud is a systemic financial risk, with 25% of fires caused by arson or suspected arson. 10% of respondents said it was acceptable to submit a false insurance claims. Medicare fraud exceeds $60 billion per year. Phony automobile and other bodily injury claims cost billions annually, and are difficult to control since it is impossible for a court to tell someone they are not in pain. Identity Theft rose 22% in 2008, to 10 million cases, a record. It takes the average victim 330 hours to repair the damage to their personal reputation Identity Theft is estimated to cost individuals and businesses $221 billion per year Each day, 175,000 phony checks are presented as payment. The cost of check fraud is estimated to exceed $50 billion annually.*

www.321gold.com/editorials/dougherty/dougherty090209.html

This *is* for real

EU Intelectual Property Criminal Measures Directive : 2007

New Cybercrime laws: updated June 2009

Thailand, Germany, Zimbabwe, S. Koreal, France (?), Saudi Arabia, Kenia, UK (ammendments), etc. www.cybercrimelaw.net/

Cybercrime Bill of laws passed by Senate (2009)

USA (Alberto Gonzales);

Brasil (Eduardo Azeredo): “e-AI.5”

Origin: Budapest Convention (nov 2001):

“*[to] provide guidelines for national legislatures concerning the definition of certain computer crimes and ... criminal procedural law connected with information technology*”

Neo-inquisition

“Strong IP” <=> Inquisition (Catholic Church's)

Internet <=> Gutemberg's press

Piracy / Sharing <=> Heresy, Blasphemy

Hackerism <=> Sorcery, Witchcraft

FOSS = Comunism, Anti-capitalism, Libertarianism <=> Satanism

Imaterial Patents + Trolls + Courts <=> Witchhunt

Fight *file sharing* + Tv, Media <=> Want to burn herectics at the stake