



RESPONSE

TO THE EUROPEAN COMMISSION'S PUBLIC CONSULTATION ON THE OPEN INTERNET AND NET NEUTRALITY IN EUROPE

Summary

The significance of the problem to observe net-neutrality becomes clearer after an examination of the evidence that the open, transparent, character of the Internet disadvantages certain governments. Evidence is easily found.

- on 26th Sep., 2010, Canadian International Trade Minister Peter Van Loan stated that RIM should be able to meet India's need to watch and control BlackBerry information flows (AFP. *BlackBerry maker closer to averting Indian ban*, Totaltelecom, Tuesday, September 28th, 2010)

As the number of governments that want to watch and control the information flows of the Internet is increasing and compelling other governments to follow suite, Swissphone's response leads into a historical perspective of watching and controlling information flows from the distinct viewpoints of the *controller* and the *controlled*.

Swissphone's purpose is to convincingly demonstrate that the object of the *controller* is to penetrate the conscience, subconscious and unconscious of the *controlled*, and that the pretence of wanting to manage services helps central controllers to attain their objective.

Key terms: Control by fear, Monopoly, Monopsony



1 THE OPEN INTERNET AND THE END-TO-END PRINCIPLE

QUESTION 1: Is there currently a problem of net neutrality and the openness of the internet in Europe? If so, illustrate with concrete examples. Where are the bottlenecks, if any? Is the problem such that it cannot be solved by the existing degree of competition in fixed and mobile access markets?

Yes there is a problem for certain governments to observe net-neutrality. For example:

- on 18th March 2010 the US Department of Homeland Security (DHS) announced it was conducting a Privacy Impact Assessment in connection with the requirement of ISPs to watch, select and redirect Internet traffic, to apply intrusion detection and prevention measures to that traffic, and for the United States Computer Emergency Readiness Team (US-CERT) to generate intrusion detection alerts¹.
- In the last three years, several governments have taken steps to watch BlackBerry information flows in the RIM (Research in Motion, headquartered in Waterloo, Ontario, Canada) system. How RIM responded to past demands from the USA² and China³, and will respond to present demands from India and the United Arab Emirates remains an open question.

As the number of governments that want to watch and control the information flows of the Internet is increasing and compelling other governments to assist them, or follow suit, Swissphone's response looks at the essential history, theory and practice of watching and controlling information flows.

QUESTION 2: How might problems arise in future? Could these emerge in other parts of the internet value chain? What would the causes be?

How the problems to watch and control information flows present themselves affects both, the way they are dealt with and the potential for future problems.

Consider, for example, how the problems to watch and control the information flows of wireless telegraphy presented themselves to the exponents of managed services attending the Preliminary Conference at Berlin in 1903 on Wireless Telegraphy:

"The object aimed at by the Propositions under Art. I. is, then, in the first place, to **prevent the creation of a monopoly in favour of a single system**, and, in the second place, to avoid disturbances of the different systems between themselves.

It is towards such a monopoly in favour of a single system that there appears to be an aspiration in one direction. By arrangements which the Wireless Telegraph Company has concluded with the British

¹ US DHS, (2010). *Privacy Impact Assessment for the Initiative Three Exercise*, March 18, 2010.

² Associated Press, (2007). *France Bans BlackBerry Use by Government Officials*, FOXNEWS, Friday, June 22, 2007.

³ The Times of India, (2010). *BlackBerry server in Chian? India wants a monitoring unit too*, July 29, 2010. 03.43am IST.

Lloyds, the latter undertakes to employ the Marconi system exclusively in its stations, and not to permit these stations to communicate with ships equipped with other systems. It has been found that Lloyds' stations, in pursuance of this principle, do not reply to calls from ships furnished with other systems. Such a provision limits in a material degree the utility of radiographic telegraphy. Nor does it better accord with the interests of technical development: wireless telegraphy is still too young to enable one to yield to a given system superiority or preponderance over all others. **Only by the free competition of the scientific knowledge and technical skill** of all nations can one hope to attain improvements and progress of which this modern branch of technical science has still need to a large degree. The German Government is of the opinion that the interests of navigation, as well as technical interests, imperatively demand that communication between shore stations and ships should be facilitated as much as possible, without regard to existing systems.

For the same reason the German Government believes it to be necessary to adopt measures to prevent, as far as possible, reciprocal disturbance between the different systems. None of the systems at present in practical use has solved in a satisfactory manner the problem of enabling two stations, of which one is within the sphere of action of the other, to communicate with a third or fourth station without dislocating the working of each other. If **the various systems must, as a matter of principle, be admitted to free competition**, it will be so much the more important to lay down certain international rules to **limit reciprocal disturbances** as much as possible." (Nelson G. R., Translation of the Procés-Verbaux and Protocole Final. *Preliminary Conference at Berlin on Wireless Telegraphy, August, 1903*. pp. 7 [emphasis added]⁴).

The historical evidence bears out that the pretence of wanting '*to prevent the creation of a monopoly in favour of a single system*', and '*to admit various systems, as a matter of principle, to free competition*', was to establish a '*single system*' without the consent of the people who were allowed to agree with it but forbidden to voice their disagreement.

By relating to the essential historical background, as well as the theory and practice of watching and controlling information flows, Swissphone hopes to convincingly demonstrate that to concentrate on the roots, devices and technique of central controllers, without regard to the social consequences of their usage is tantamount to selling our remaining freedoms for a "pottage of lentils".

⁴ The complete *Procés-Verbaux and Protocole* of the Preliminary Conference is available at: <http://www.itu.int/en/history/radioconferences/Pages/1903Berlin.aspx>.

QUESTION 3: Is the regulatory framework capable of dealing with the issues identified, including in relation to monitoring/assessment and subsequent enforcement?

The regulatory framework is quite beside the point.

Thirty years back, the novelty of the Internet was represented by the fact that its inventors interpreted the problem of passing information indirectly as a send-receive problem only. In this sense they left out from their analysis both the intermediating networks and the problem of contriving to watch and control all information flows in order to identify users, measure call holding times and make meticulous bills. And yet, the focus of the regulatory framework is on the intermediating networks and the problems of watching and controlling information flows.

By characterising the problem to pass information indirectly as a traditional *telecommunication* problem the regulatory framework perpetuates a bad precedent. An entirely different mode of thinking needs to be deployed.

2 TRAFFIC MANAGEMENT/DISCRIMINATION

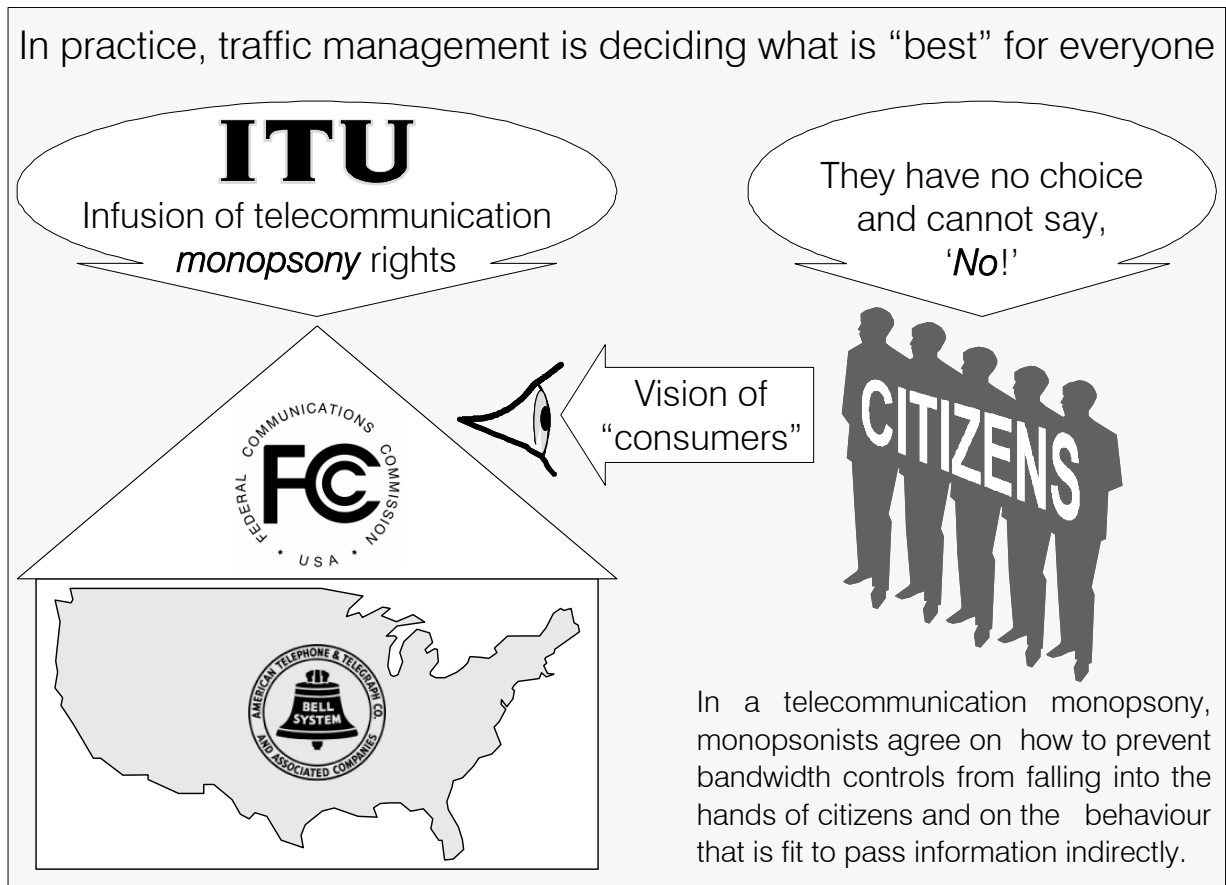
QUESTION 4: To what extent is traffic management necessary from an operators' point of view? How is it carried out in practice? What technologies are used to carry out such traffic management?

Traffic management is, from the view point of the exponents of managed services, necessary in order to prevent bandwidth controls from falling into the hands of the controlled.

The practice is carried forward by telecommunication criteria which are united in the *monopsony* formed under the word '*Telecommunication*' defined at Madrid, in 1932, by the International Telecommunication Union (ITU) as; '*Any telegraph or telephone communication of signs, signals, writings, images, and sounds of any nature, by wire, radio, or other systems or processes of electric or visual (semaphore) signalling.*'

monopsony	a market situation in which one buyer exerts a disproportionate influence on the market. Greek <i>mon</i> single + <i>opsonia</i> purchase of victuals, from <i>opson</i> food + <i>oneisthai</i> to buy.
------------------	--

Under this nonsensical, but decisive, definition, monopsonists, as the only buyers of bandwidth controlling technology not sought by anyone else, have the right to determine what human behaviour is fit or adapted to pass information indirectly.



To be correct, we have to recall that before 1932, some indirect information-passing organisations were quite distinct and arranged along entirely different lines of control like those of the Western Union and Bell Company, but eventually they were united into a single, “universal service”, system.

Perhaps monopoly was for the “best” in the 1930s. Monopsonists, then, only had one end-to-end product; telephony, so custom requirements were beside the point. The *controlled* were being controlled to use telephones only.

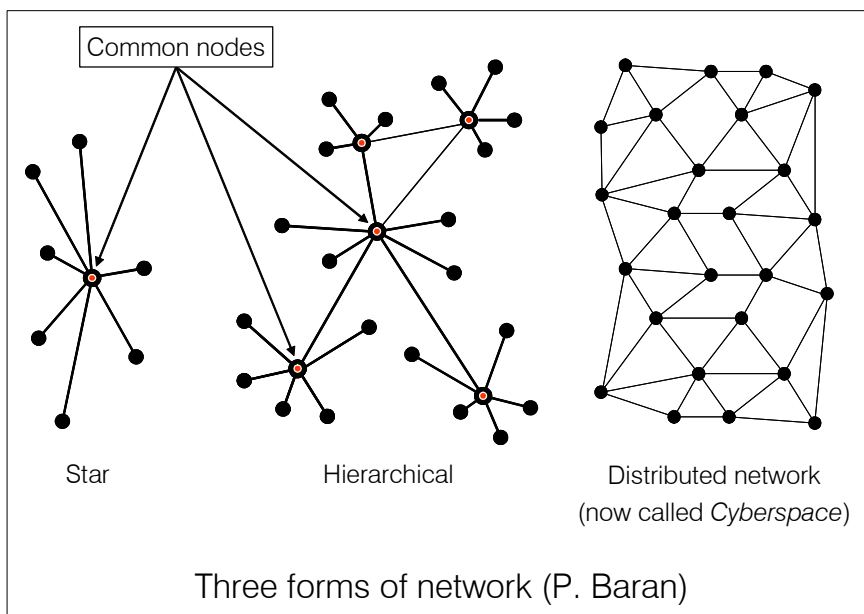
But telephones are unsuitable for numerous intimate needs. For a case in point that what is “universally”, technically (and legally) feasible does not meet innumerable custom requirements, look at the development of the Internet.

CUSTOM REQUIREMENTS ARE BASED ON HOW PROBLEMS PRESENT THEMSELVES

During the 1960s, the body politic in the United States (US) is convinced that it would be difficult to command a counter attack in case of a nuclear strike by the Union of Soviet Socialist Republics (USSR). One of the main concerns is the common nodes in AT&T's centrally controlled networks.

Centrally controlled networks are either *star* or *hierarchical* networks. A star network dies if its common node breaks down. In a hierarchical network, the destruction of only a few common nodes suffices to make indirect information-passing impossible.

According to Paul Baran⁵ of the RAND Corporation, the solution lies in building a "distributed" network that allows data to circumnavigate any parts destroyed by enemy



attack, and the concept put into practice is the transparent Internet in *Cyberspace*.

Incidentally, the Internet is proof that accidents will occur in the best-regulated families.

'Families' is used here in a loose, general, sense with reference to institutions such as the ITU, FCC and AT&T,

etc., as I am, of course, alluding to the quite unexpected arrival of information flows that escape the control of central controllers – See, box below.

⁵ Baran, Paul. (2002). The Internet: Past, Present, and Future - The Beginnings of Packet Switching: Some Underlying Concepts. *IEEE Communications Magazine*, July 2002, pp. 42-48.

"And finally, Phil Enslow, from OTP talked about what the FCC thought was regulated and was not, and how the ARPA net didn't fit in their picture of the world. He also mentioned that, in his opinion, the one thing that would make AT&T most unhappy was transmitting voice over the ARPA net."

Bob Barker, Memorandum to IMP project team, 8 June 1972

OTP	White House Office of Telecommunication Policy
FCC	Federal Communication Commission (US regulator of interstate and international telecommunication)
ARPA	Advanced Research Projects Agency
IMP	Interface Message Processor (Part of ARPA's computer network project)

Cyberspace is the environment in which information is processed and transferred either with or, if transiting the Internet, without reference to any telecommunication criteria.

How the custom requirements of the US Department of Defense (DoD) affected the design of the Internet is clearly and precisely described in "The Design Philosophy of the DARPA Internet Protocols⁶" by David Clark of the Massachusetts Institute of Technology.

In the past, custom requirements, however, have depended on one set of conditions, and now another, and so we should not be surprised if the current open, transparent⁷, character of the Internet changes over time.

In any event, Swissphone recommends "The Design Philosophy of the DARPA Internet Protocols" as well as Clark's other seminal paper with Saltzer et al., "End-to-End Arguments in System Design⁸", as these two papers provide valuable guidance on the relationship between cause and effect which is, of course, material to the European Commission as cyberspace is increasingly characterised by custom design networks of which the Internet is at once the principal representative and common denominator.

⁶ Clark, D.D. (1988). The Design Philosophy of the DARPA Internet Protocols, *Proc SIGCOMM 88, ACM CCR* Vol. 18, Number 4, August 1988, pp. 106-114, Available at:

<http://groups.csail.mit.edu/ana/Publications/PubPDFs/The%20design%20philosophy%20of%20the%20DARPA%20internet%20protocols.pdf>

⁷ For a concise description of the current transparent character of the Internet see: Carpenter, B., (2000). *Internet Transparency*, RFC 2775. Available at: <http://www.ietf.org/rfc/rfc2775.txt>

⁸ C Saltzer, J.H., Reed, D.P. & Clark, D.D. (1984). End-To-End Arguments in System Design, *ACM TOCS*, Vol. 2, Number 4, November 1984, pp. 277-288 available at: <http://www.cs.wisc.edu/~bart/739/papers/end-to-end.pdf>

FOUR GENERAL OBJECTIONS TO THE PRACTICE OF TRAFFIC MANAGEMENT

Following on immediately from the foregoing, the four general objections to the practice of traffic management are that it:

1. is carried forward by a monopsony that – in the long run at least – behaves in a self-assertive manner to impose its own laws and behaviour-controls,
2. severely constrains the freedom to access information, choose the most practical way of relating information to effective action, and to innovate. (NB. At the end of the 20th Century these three constraints were major determinants of change),
3. is quite insensitive to how intimate information problems present themselves to us, which appears to be a basic mistake of method in seeking to regulate information flows.
4. is increasingly disrupted by custom designed networks. This does not imply that the custom designed networks disrupt information *flows*. Rather, it is that newly proposed telecommunication criteria such as, for example, IP-Traceback⁹ and International Caller-ID cannot be applied now to TCP/IP without disrupting custom designed networks, intruding in our private lives and seriously complicating all other indirect information-passing matters to the extreme.

QUESTION 5: To what extent will net neutrality concerns be allayed by the provision of transparent information to end users, which distinguishes between managed services on the one hand and services offering access to the public internet on a 'best efforts' basis, on the other?

Since proposals to watch and control information flows are from the viewpoint that notwithstanding the obvious advantages of the Internet, it presents several disadvantages to the exponents of managed services, it may be appropriate:

1. to review, briefly, the disadvantages of the open, transparent, character of the Internet,
2. to comment on the subject of information management in general, and
3. to consider the threat to an open society from the managed services.

⁹ Basic Information on the ITU-T IP-Traceback and International Caller-ID Capability Initiatives. Available at: http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/Rutkowski_IPtraceback_callerID_rev0.pdf

DISADVANTAGES OF THE OPEN, TRANSPARENT, CHARACTER OF THE INTERNET

The ITU Secretariat, in its document "Beyond Internet Governance"¹⁰ to the World Summit on the Information Society at Geneva in 2004, could write in these words on the major concern about the Internet Corporation for Assigned Names and Numbers (ICANN) and the management of Internet resources in general:

Put simply, many of the debates on management of Internet resources center around whether the Internet should be loosely coordinated by a private corporation, or more formally overseen; who should coordinate or oversee such functions, and the exact role of different actors, including governments, the private sector and civil society.

In particular, a topic of key concern to some representatives of civil society appears to be that Internet governance should transcend national boundaries and not be subject to the ultimate authority of nation states. That is, a governance model is envisaged (but not yet articulated clearly) that would be the antithesis of the model embodied in traditional intergovernmental organizations based on the primacy of national sovereignty. (p. 10)

Clearly, the suggestion of a model of governance '*that would be the antithesis of the model embodied in traditional intergovernmental organisation based on the primacy of national sovereignty*' from the ITU, which is the UN agency for information and communication technologies, requires special consideration because it represents at once not only the creation of an Internet Governance monopsony, but the eventual eyes, ears and mouth of a single world government also.

Four further disadvantages are that the Internet does not offer any means:

1. to prioritise traffic,
2. to determine throughput times,
3. to implement bandwidth controls, and
4. to charge users on a traffic payload basis.

These four disadvantages are, however, conditional and not fundamental in that they have not, and do not, prevent the spread of open, transparent, connections to everything digital.

Generally speaking, the practice of controlling bandwidth in order to charge, bill and collect for opening a connection path is an important and honourable practice. But it is deficient in its application to information flows in that it considers neither the consecutiveness of the

¹⁰ Document available at: http://www.itu.int/council/wsis/Geneva3_04/intgov-contribution-wg-wsis.doc.

plenipotentiary governance that is required to perpetuate it, nor how crucial information problems present themselves to us, nor the custom requirements of users, nor the continuous progress of technology.

Clearly, the pretence for managing services is to introduce and maintain "solutions" that are neither autonomous nor flexible and in consequence custom design networks are not here out of mere fancy but because of requirements that are genuine.

COMMENT ON INFORMATION MANAGEMENT IN GENERAL

The subject of information management needs a completely fresh examination because it is based on the received wisdom that information flows are logically, and technically, controllable when, actually, they are not.

The two gravest dangers that we face due to this received wisdom must be considered. First, there is the danger that we continue to incorrectly assess what human beings and modern technology can do in cyberspace.

Cyberspace is, in effect, new information and innumerable new connections and disconnections each *picosecond* some of which escape control. Likewise power outages, nuclear energy and synthetic chemicals, a frenetic biological and agricultural trade, etc. are borderless and can easily escape control also.

Antivirus software, sensible concealment of passwords, etc. are necessary precautions in cyberspace but it is hard to tell what such 'security measures' actually do and in any event, no country has a way to safeguard itself from information that may be corrupted by error or malice in a computer (or person) working in connection with, for example, a major power plant. We see this time and time again with disruptions such as in Italy in September 2003, in the Northeast American Blackout a month before, and so on, since the nuclear accident at Three Mile Island in 1979.

Second, there is the danger of using discredited methods. The two main features inherited from the 20th century are agnosticism and terror. Both are closely allied for only where faith has disintegrated does tyranny prosper and spread terror.

Following the collapse of Christianity in Germany, antichrist and mass psychologist Adolf Hitler, in 1927, could declare:

"The masses are but a part of Nature herself. Their feeling is such that they cannot understand mutual hand-shakings between men who are declared enemies. Their wish is to see the stronger side win and the weaker wiped out or subjected unconditionally to the will of the stronger" (Mein Kampf, Adolf Hitler, Translated into English by James Murphy, pp. 281).

After Hitler, waves of unassailable "facts" and the Cold War urged agnosticism and terror to embrace the whole East-West axis.

The common denominator of agnosticism and terror is fear. The 20th Century has clearly shown that control by fear can become a decisive, rational instrument for the establishing and maintenance of a dictatorship.

Control by fear

'The advisory system is based on five threat conditions or five different alerts: low, guarded, elevated, high and severe,' said Director Ridge. 'it empowers government and citizens to take actions to address the threat.' (White House photo by Paul Morse, March 12, 2002).

Using discredited methods for promoting confidence in the central controller's "better" judgements and the ascendancy of uniformity.

Fear is inappropriate for deciding on the course of action that is best and it worsens the crisis in which nations find themselves when they are already centrally controlled.

THREAT TO AN OPEN SOCIETY FROM CONTROL BY FEAR

Before we take the drastic step to watch and control the information flows of an open society, we need to remind ourselves that a path is not the same thing as a connection. Grandma and her grandchildren are connected regardless of whether or not there is a path between them. A path is what is used by information to get from one point to another. A path is a feature of a connection.

The word 'path' is used for trajectories taken by disembodied information, e.g. radio propagation path, or *transparent* path which is for a connection that persists a long time¹¹. In which case, it cannot be too clearly emphasised that taking steps to watch and control the information flows of the Internet, carries very grave risks.

Even so, arch-rhetorician Tom Ridge in his keynote speech at the 71st APCO International conference in 2005, stressed that the most important ambition of the USA is to watch and control all interstate and international information flows – We've been there before¹², No?

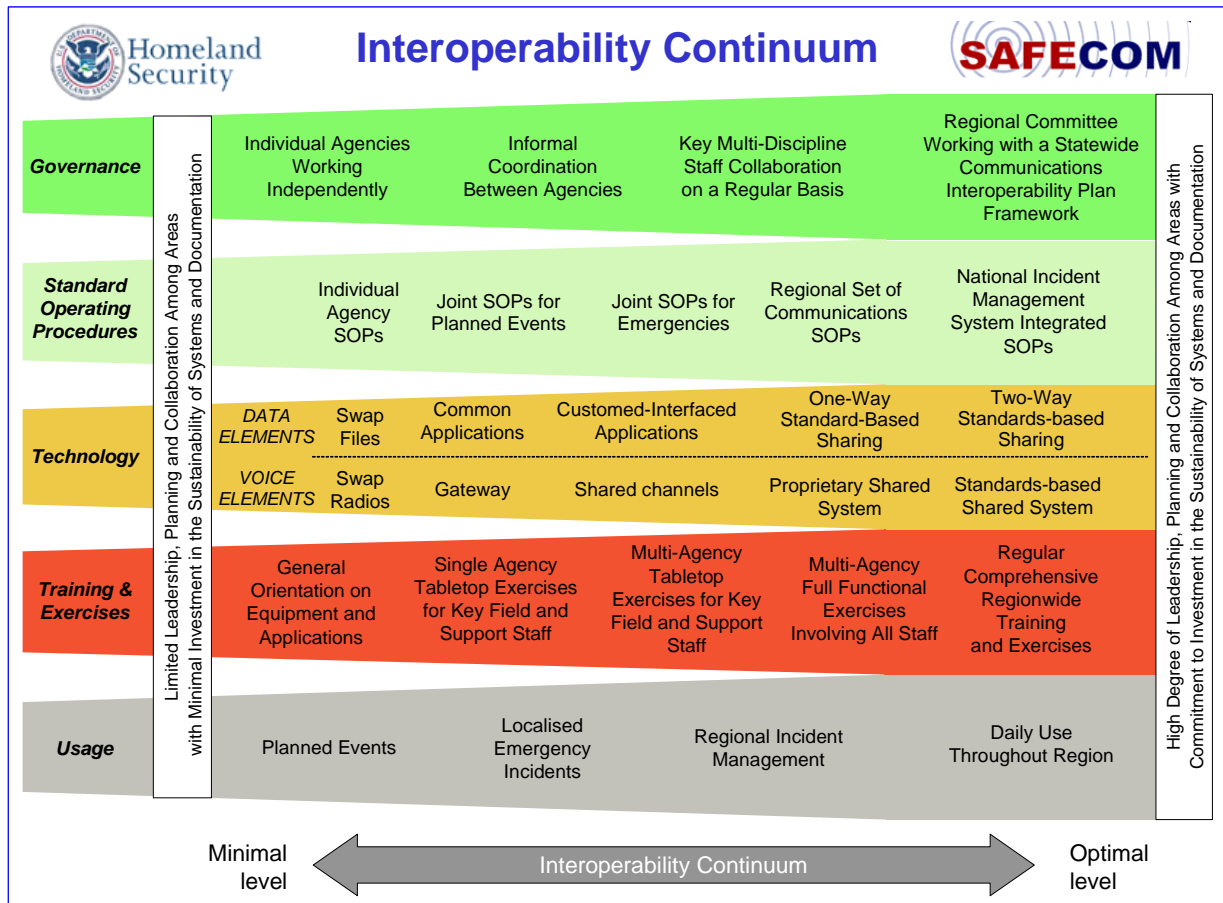
As the first Security Secretary of the US, Tom Ridge stated that the Department of Homeland Security (DHS) was established to combat terrorism around six convictions:

1. Risk cannot be eliminated; it must be managed.
2. We need to integrate the country; everyone must work together (implies central control and planning).
3. People and technology must be integrated: people + technology is $1 + 1 > 2$
4. No security system should depend on a *single point of failure* [sic] that brings the entire system down when it fails.
5. Protection requires the interlocking of four sophisticated technologies: those of detection, identification, authentication and connection (i.e., record keeping)
6. To avoid crippling the economy, there must be a way of keeping doors open when borders are closed.

¹¹ Loosely speaking: Complete transparency - complete memory/record; partial transparency - partial memory/record; no transparency - no memory or no record.

¹² The lessons to be drawn from Mussolini's Italy, Hitler's Third Reich and Stalin's Soviet Union, and from the pursuit of the Cold War by the United States, are that the control of information – and, therefore, of a nation as a whole – requires rhetoric (i.e., propaganda) and central supervision, and that watching and controlling information technologically – or by any other means for that matter – is a hazard itself.

Although Tom Ridge did not say how the convictions of the DHS were generated, the message to the audience was unequivocal: central control is indispensable to the US! Everyone in homeland security¹³, therefore, must henceforth weave these six Homeland Security convictions by referring to the Interoperability Continuum of the DHS.



Interoperability Continuum¹⁴ - Guidance to merge the distinct agendas of myriad local governments into the single agenda of a strong central controller.

¹³ Homeland Security leverages resources within federal, state, and local governments, coordinating the transition of multiple agencies and programs into a single, integrated agency focused on protecting the American people and their homeland. More than 87,000 different governmental jurisdictions at the federal, state, and local level have homeland security responsibilities. The comprehensive national strategy seeks to develop a complementary system connecting all levels of government without duplicating effort. Homeland Security is truly a "national mission." Downloaded on September 16, 2010, from: <http://www.dhs.gov/xabout/structure/>

¹⁴ Available at: http://www.safecomprogram.gov/NR/rdonlyres/54F0C2DE-FA70-48DD-A56E-3A72A8F35066/0/Interoperability_Continuum_Brochure_2.pdf

Since it urges central control and gives uniformity precedence of right over plurality on the one hand, and since it infers that only organisations which are officially recognised are capable of keeping the public safe and secure, and since it is technically and logically possible to control information fully on the other hand, the Interoperability Continuum of the DHS – which is mimicked by the UK and several other European countries – is the perfect recipe for alienating the power of independent judgement. But what can anyone say against making Homeland Security flawless?

QUESTION 6: Should the principles governing traffic management be the same for fixed and mobile networks?

The question is: Why should they be different? Wireless connectivity is the most desired indirect information-passing feature on the planet and, presently, Smartphones, Laptops, Tablets and other broadband wireless gadgets are fundamentally changing the way *distributed processing* works; soon *distributed processing* will define local in global, instead of global in local.

The trend is consistent with the tradition that wireless connectivity is matched to fixed connectivity. The match, however, requires license-exempt spectrum optimised for broadband to be used such that wireless connectivity:

1. is established by ends using only information that is available locally, without the help of any common node,
2. makes short and long range hops,
3. decreases the information throughput whenever it is necessary to increase range, and
4. is used for *transit* or terminating/originating traffic and not just for uplink/downlink.

These features mean that the terminals actually make the network by themselves, quickly, and as they go along.

EARNING GOODWILL

The GSM Government is warning “data users” that they get what they pay for¹⁵. At circa CHF 0.20/SMS, most *feel* they don't get much and this, plus the fact that mobile connectivity uses personal information intensively, does not earn the GSM Government –

¹⁵ Lenninghan M., (2010). “Data users get what they pay for – Vodafone CEO: Colao sees more segmented and tiered mobile plans ahead; predicts end of ‘free-ism culture’ in apps”. *Total Telecom*, Tuesday 14 September 2010.

or any other government for that matter – any goodwill. Rather, it increases the demand for licensed-exempt spectrum which is suitably defended against capture by rapacious spectrum auctioneers and monopsonists in the GSM government.

QUESTION 7: What other forms of prioritisation are taking place? Do content and application providers also try to prioritise their services? If so, how – and how does this prioritisation affect other players in the value chain? No comment at this time because *prioritisation* is a subject of on-going research.

QUESTION 8: In the case of managed services, should the same quality of service conditions and parameters be available to all content/application/online service providers which are in the same situation? May exclusive agreements between network operators and content/application/online service providers create problems for achieving that objective?

The question conflates *monopsony* and *monopoly*.

It is absolutely necessary to distinguish between the two. Monopsony is a monopoly of *demand*. An indirect information-passing monopoly is the *symptom* of a monopsony.

BASICS OF MANAGED SERVICES AND SELF-ORGANISATION



MANAGED SERVICES

Managed Services rest on a central authority, or monopsony, which determines who can generate information, on what criteria and for what ends.

Technology is *policy-driven*.

Element of constitution: **Monopsony**.



SELF-ORGANISATION

Self-organisation rests on people who determine themselves how information is generated, on what criteria and for what ends.

Technology is *demand-driven*.

Element of constitution: **Gaps in information**.

QUESTION 9: If the objective referred to in Question 8 is retained, are additional measures needed to achieve it? If so, should such measures have a voluntary nature (such as, for example, an industry code of conduct) or a regulatory one?

If the objective is retained, the present course of relevant European policy will be reversed and central controllers and their accomplices will become more emboldened not to observe the complete inviolability of net-neutrality in commonplace infrastructures.

3 MARKET STRUCTURE

QUESTION 10: Are the commercial arrangements that currently govern the provision of access to the internet adequate, in order to ensure that the internet remains open and that infrastructure investment is maintained? If not, how should they change?

Neutrality is a behaviour-control criterion which has always been a ruling factor in international and national telecommunication regulation. Today, however, the meaning of neutrality, in its application to the Internet and the rest of cyberspace, varies from one country to another and even within the country it is discussed.

But, in general, without assuming neutrality can be fully understood – the idiosyncrasies of local, personal experiences prevent that – observing the complete inviolability of net-neutrality in commonplace infrastructures affords the most reliable guidance to investors¹⁶ and national security.

4 CONSUMERS – QUALITY OF SERVICE

PEOPLE – BENEFIT OF PLURALITY

GENERAL REMARK: Like all previous questions, the questions in this section are answered from the point of view that the core issue is one related to *plurality* rather than to “transparency and quality of service”.

¹⁶ The overall effect of contriving to watch and control information flows is negative, not positive and, according to AT&T, ‘telecommunication’ is simply not the future of cyberspace. In 2005, the CEO of AT&T wrote; “IP technologies were fundamentally changing the way that businesses of all sizes were managing their operations. Wireless siphoned off revenues from wireline services. E-mailing became a popular substitute for phoning. Customers were leaving. Prices were plummeting. It was ugly.” (Dave Dorman, Chairman of the Board & CEO of AT&T, (2005). *Transformation – The story behind AT&T's reinvention*, March 2005).

QUESTION 11: What instances could trigger intervention by national regulatory authorities in setting minimum quality of service requirements on an undertaking or undertakings providing public communications services?

It is important to consider first that there are always gaps in information as well as notions of what is fit to the continuous struggle of obtaining missing information and, then, that to set quality of service requirements with notions about people and information that are groundless endangers prosperity and ultimately both life and country.

QUESTION 12: How should quality of service requirements be determined, and how could they be monitored?

Quality of service has to do with how missing information is obtained, not with how things work or how information problems are re-interpreted.

The problem of obtaining missing information is as old as life itself but, in the last thirty years, the general problem of obtaining missing information has changed radically, both in its nature and in its range and, despite the technological wonders of today, it is fair to say that it is more acute than it was ever before.

For this there are a number of reasons. From a communication regulation perspective, the most important is that very little, not to say no, consideration is given to how information problems actually present themselves to people. In spite of the great amount of work that has been carried out on the subject of passing information safely and securely since Shannon¹⁷, there is still a need for much more research into what can pass information indirectly without obscuring valid perceptions and this in such a way that it will be safe to assume that the procedure is of *service* instead of a *disservice*.

QUESTION 13: In the case where NRAs find it necessary to intervene to impose minimum quality of service requirements, what form should they take, and to what extent should there be co-operation between NRAs to arrive at a common approach?

It is not unusual, especially during the early stages when practice is not guided by existing knowledge derived from research, that intervention suppresses the symptoms without treating the condition. This often is the case, for example, in the medical profession where

¹⁷ C. E. Shannon (1948). *A Mathematical Theory of Communication*. The Bell System Technical Journal, pp 379 – 423, July 1948 No.3, and pp. 623 – 657, October 1948 No.4 Vol. XXVII.

recent discoveries arrived at through decades of research underscore the fact that sound medical practice is beyond the competence of many doctors and nurses.

The point is that compared to the mysticism of communication, the material of organisms is a model of simplicity and that Communication Regulators, therefore, cannot hope to have the competence that is required to intervene effectively without guidance from knowledge that is derived from decades of research.

It is not a state secret that, since the early years of radio to the present time, regulatory intervention has been guided by information about people, life-and-death situations, technology and communication that is *groundless*. This historical fact means that in the absence of any concrete research-based knowledge of what communication includes, the goal set by the Commission in 1983 to arrive at a “legal framework which is *clear* and *precise*¹⁸” is not around the corner; in the meantime, it would be better to focus on satisfying demands to pass information indirectly based on how passage is guided by gaps in information.

QUESTION 14: What should transparency for consumers consist of? Should the standards currently applied be further improved?

Integrity.

There is no integrity where “transparency” can be “further improved”.

5 THE POLITICAL, CULTURAL AND SOCIAL DIMENSION

QUESTION 15: Besides the traffic management issues discussed above, are there any other concerns affecting freedom of expression, media pluralism and cultural diversity on the internet? If so, what further measures would be needed to safeguard those values?

Two major concerns are *mode* of expression and the trend towards *uniformity*.

¹⁸ A Community political and legal framework, which is *clear and precise*, thus becomes indispensable A legal framework does not imply, however, additional constraints and bureaucracy; on the contrary, it will quickly become apparent that the gradual transfer of power and resources to the Community, *if brought about as the Commission envisages*, will be counterbalanced by a *reduction in regulations* and, moreover, a more rational utilization of public resources allocated to this sector. (Commission of the European Communities, COM (83) 329 final, Brussels, 9th June 1983. p.10; [emphasis added]).

THE BIGGEST CHALLENGE COMMUNICATION REGULATORS FACE

Ironically, the biggest challenge communication regulators face will be to develop gradually an aversion to specialised language that gives the pretence, but not the reality, of meaning.

Indeed, we now know that the use of terms like “monopoly” and “free competition” in a general, speculative and dogmatic way is sure to be followed by catastrophic consequences.

6 ANY OTHER ISSUES

THE OBJECT OF COMMUNICATION REGULATION

In general, communication regulation recognises no boundary; it regards total ubiquity as its rightful territory. Indeed, the focus of communication regulation is UNIVERSAL SERVICE. It deals with “minimum connection” requirements. Neither the child nor the adult is considered; only the eligible object, the abstract unit of the terminal user is in evidence.

In the abstract, unit person and terminal are equal; both universality and central control demand equality. Such equality is consequently guaranteed by communication regulation which is calculated by central controllers to assure the triumph of logic over morality. But the defeat of morality reconstitutes people as it affects the way people think or alters the conditions under which thinking is permitted. Equality reduces indigenous judiciary systems into a state of dissolution and local disintegration with the consequence that the law focused on faith, private property, territoriality and the mysticism of its inhabitants is gradually destroyed.

Thus, we see that the object of communication regulation is to open the way for a central controller to penetrate the conscience, subconscious and unconscious of every human being, and that the pretence of wanting to manage services is to help attain that objective.

* _ * _ *

Edouard Dervichian

Swissphone Telecom AG

<http://www.swissphone.com>

Contact: edouard.dervichian[at]swissphone.com