Project Number:	**FP7-257123**
Project Title:	**CONVERGENCE**
Deliverable Type:	**Report**
Dissemination level	**Public**
Deliverable Number:	**D.8.5**
Contractual Date of Delivery to the CEC:	**Month 33 (amended to Month 35) 30.04.13**
Actual Date of Delivery to the CEC:	**14.04.2013**
Title of Deliverable:	**Report on potential social and economic impact**
Work package contributing to the Deliverable:	**WP8**
Editor(s):	**Richard Walker (XIW)**
Author(s):	**Richard Walker (XIW), Barbara Benincasa (XIW), Raffaele Di Fuccio (XIW), Andrea Pede (XIW)**
Abstract:	**This report explores the possible social and economic impact of ICN and of CONVERGENCE. We explore the way in which the new technologies could affect ongoing "tussles" between Information Providers and Information Consumers. We conclude that they have the potential to affect multiple dimensions of economic social and political life, with different effects on different actors. Whether the net effect on the public good would be positive or negative is impossible to predict. CONVERGENCE– like other research projects – has created new "possibles" – building blocks for future development. How they will be used is and must be an open question.**
Keyword List:	**Impact, ICN. CCN, regulation, tussles**

Executive Summary

The goal of this report is to discuss the social and economic impact of the technologies and concepts developed by the CONVERGENCE project – and of Content-centric networking or Information-Centric Networking (ICN). The practical and ethical problem is that the published literature provides very little evidence supporting the value of this kind of assessment. Indeed, it has been argued, persuasively, that nearly all such forecasts are false. The content of the report is guided by the authors' awareness of this criticism.

The report begins with a brief introduction to Information-Centric Networking and CONVERGENCE, introducing the conceptual distinction between content-centric and source-centric packaging of information. The current architecture of the Internet is based on a source-centric model. ICN, by contrast adopts a content-centric model, in which the fundamental units of transaction are "named data items", protected by content-centric security. CONVERGENCE extends this concept, introducing ideas from the MPEG community – in particular the possibility of bundling named data items with metadata, a scheme allowing owners of VDIs to define and enforce licenses, and functionality allowing owners to monitor the use of VDIs.

The report goes on to discuss how the introduction of ICN and CONVERGENCE technology could affect "tussles" (conflicts) about the way the Internet is used.

- Who can provide commercial and non-commercial content to other users
- Who can monitor and or control the information that users provide to other users
- What content we want and what we get
- What we need to expose in order to get what we want
- Who "owns the user experience"

In each case, we contrast the social and economic implications of the current Internet with possible changes induced by the widespread adoption of ICN and CONVERGENCE. The discussion covers some changes that many readers would regard as beneficial and others likely to less welcome. We argue that widespread uptake of the new technologies could strengthen the economic and political role of Information Providers with respect to the large centralized services that dominate the current Internet economy. At least in theory, the change could extend from large corporate providers of information (e.g. newspapers) to the individual users who feed services like Facebook, Instagram and Flickr. This could have a positive impact on the ability of Information Providers to earn a living from their work and on the quality and quantity of information available to end-users. However we also suggest that the new technology could reduce access to information for countries and individuals who cannot afford to pay for it, and reduce the diversity of views available to users. CONVERGENCE could make it harder for web sites to collect information that users wish to keep private and

support digital forgetting but it could also make it harder for political dissidents to maintain their anonymity on the network.

In the following chapter we review major obstacles to uptake, in particular the need to modify routers across the world, the broad range of actors who benefit from the current architecture of the Internet, consumer conservatism, and network effects. However we suggest that the current trend towards domination of the Internet economy by a small number of very large companies has reduced its "robustness" against unexpected technical, economic and political events and that this fragility could create opportunities for new technologies. We also suggest that there exist significant opportunities for niche applications: "islands of innovation" that do not require wholesale change in the architecture of the Internet and which could seed future revolutionary change.

We conclude that the new technology has the potential to affect multiple dimensions of economic social and political life, with a net effect on the public good that is impossible to predict.

CONVERGENCE– like other research projects – has created new "possibles" – building blocks for future development. How they will be used is and must be an open question.

INDEX

TERMS AND DEFINITIONS

TERM	DEFINITION
CoMid	The CONVERGENCE Middleware Level.
CoNET	The CONVERGENCE Network Level.
Content-Centric networking	A network concept, introduced by van Jacobson [1] in which the fundamental unit of transaction is a “named data unit”
Information-Centric Networking	Synonymous with Content Centric Networking (see above)
IPR	Intellectual Property Rights
License	In CONVERGENCE, a machine-readable expression of Operations integrated in a VDI, that asserts the terms and conditions under which a user can use the VDI. A subset of these terms and conditions is directly enforced by the CoMid and the CoNet
Rights Expression Language (REL)	A language allowing the owner of a VDI to express a license.
Versatile Digital Item (VDI)	A structured, hierarchically organized, digital object containing one or more resources and metadata, including a declaration of the parts that make up the VDI and the links between them.

Table 1: Terms and definitions.

1 Prediction is difficult

The goal of this report is to discuss the social and economic impact of the technologies and concepts developed by the CONVERGENCE project – and of the class of technology to which CONVERGENCE belongs: Information-centric, or Content-centric networking [1, 2]. Before embarking on the main discussion, a methodological discussion is in order.

All project proposals in the Framework 7 Program contain a mandatory section on "impact", in which authors are supposed to explain how their research will improve, or ideally "transform" European society and the European economy. The score for this "impact section" helps to determine the overall score given to the project during evaluation and its chances of receiving funding. Many projects, including CONVERGENCE, also plan a deliverable on "social and economic impact". This is because the partners believe, rightly or wrongly, that the inclusion of such a deliverable will improve their project's chances during the selection process.

The practical and ethical problem is that the published literature provides very little evidence supporting the value of this kind of assessment. Indeed, Nassim Nicholas Taleb [3, 4] has argued, on empirical grounds, that nearly all such forecasts are false. S. Kauffman [5] provides theoretical arguments supporting this view. According to Kauffman, every biological and technological innovation creates opportunities for further innovation; unfeasible ideas become feasible; old technologies find new applications, inventors discover new challenges. In brief, the evolutionary process follows a single trajectory across a potentially infinite space of "possibles". Since forecasting can only explore only a tiny region of this space, the probability that it will identify the region corresponding to the state of the system at a given time in the future is vanishingly small. Extra effort is little help. Like other combinatorial problems, the difficulty of forecasting scales exponentially [6].

This report will be guided by the authors' awareness of these limitations. We will therefore adopt a number of methodological precautions.

- We will make no attempt to systematically explore the complete space of possible technology developments and their impact on society. Rather we will focus on a small set of major societal and economic issues, likely to be of interest to a broad readership. In particular, we deliberately avoid discussion of the impact of ICN on the internal structure of the telecommunications industry. On this issue we refer readers to the excellent discussion in [7].
- We will adopt a discursive approach: for each of the issues we discuss we will compare ICN and CONVERGENCE-based solutions to the current architecture of the Internet, identifying the advantages and disadvantages from the point of view of

different actors and values. Whether or not the advantages outweigh the disadvantages or vice-versa is an issue we will leave to the judgment of the reader.

- Except in case in which a particular result seems completely implausible, we will not discuss the probabilities of different outcomes.

Two simplifying assumptions will guide our presentation. The first optimistic, or "half glass full", assumption is that ICN and CONVERGENCE will perform as advertised, that technological promises will be maintained. If this were not so, this report would have no point. The second "half glass empty" assumption is that the proponents of new technologies know no more about the future of society than anyone else. Our attitude to promises of economic and social impact will thus be sceptical.

The rest of this report will be organized as follows. Chapter 2 will review certain limitations of the current architecture of the Internet, describe how ICN addresses these problems and outline the novelties introduced by CONVERGENCE. Chapter 3 – the core of our study – examines the possible impacts of ICN and CONVERGENCE on "tussles" among and between different categories of Information Providers and Information Consumers. Chapter 4 concludes, identifying factors favourable and unfavourable to the take-up of ICN and discussing the implications for the public good.

2 Information-Centric Networking and CONVERGENCE

2.1 Information packing before the Internet

Schematically, we can distinguish two modes of packaging information that pre-date the Internet.

- *Content-centric packaging (our terminology). Information Providers* created packages of homogeneous information (e.g. a scientific paper, a book, a CD, a DVD, a film), which they gave, lent or sold to *Information Consumers.* The scarcity of appropriate distribution channels meant that specialist information providers had very small markets and that barriers to entry for competitors (small publishers, independent artists etc.) were strong. The limitations of distribution channels meant that many potential consumers had no access to the products theoretically on offer.
- *Source-centric packaging. Information Providers* brought together different items of information (e.g. magazine articles, news reports, books on different subjects) into an *information container* (e.g. a magazine, a news program, a bookshop, a library). New kinds of container improved consumers' access to information. However, they did not make it easier for small information providers to reach consumers. In most cases, consumers took all their information from a single source (e.g. a single news channel, a single newspaper) or from a very small range of sources.

2.2 The Internet and the World Wide Web

> *"The problem networking aimed to solve was resource sharing — remotely using scarce and expensive devices like card readers or high-speed tape drives or even supercomputers. The communication model that resulted is a conversation between exactly two machines, one wishing to use the resource and one providing access to it. Thus IP packets contain two identifiers (addresses), one for the source and one for the destination host, and almost all the traffic on the Internet consists of (TCP) conversations between pairs of hosts."*
>
> *Van Jacobson, 2009 [2]*

The architecture of the Internet – and the World Wide Web, which grew up on top of it – naturally favour a source-centric model of information packaging. Hosts (in the Web, Web servers) act as information containers. To find information on the Web, the user identifies the host where the information resides and requests the information from the host. The lower levels of the IP stack (content-neutral bit transport services) support this process. Intermediate nodes between the origin and the destination of a request know nothing about the information they are transporting. It is this model that explains the Internet's extraordinary success, and

also its weaknesses. Some of these weaknesses reflect broad social, economic and political concerns we will discuss later in this report. Others are more technical.

- When a user is interested in a specific *item of information* (e.g. a book, or a song, or a scientific paper), the architecture of the Internet forces her to search for the *source* of the information and access the source before accessing the information itself. For example, when the author wishes to download a scientific paper he typically (i) searches for the paper with Google Scholar; (ii) clicks on the link to the paper, which points to the site of an academic publisher; (iii) opens his university VPN to gain access to the site; (iv) downloads the paper; (v) downloads the citation to the paper to his citation manager. This is a slow and inefficient process.
- The bit-transport layer that carries content from source to destination is unaware of the content it is transmitting. To cache content for later distribution to other users or to offer different Quality of Services to different classes of content (e.g. video, VOIP) operators have to use proprietary CDN and deep packet inspection.
- The protection of sensitive information depends to a very large extent on authentication of hosts and clients and on encryption of the information they exchange. Once information has arrived on a host site, security relies entirely on the mechanisms put in place by the site itself. The majority of large-scale security breaches occur when attackers breach these mechanisms and gain access to unencrypted data on host servers.
- Reliance on a tiny set of information hubs creates a potential source of systemic fragility. While disaster planning and redundancy can reduce vulnerability to accidents, natural disasters and military attack, it is less effective against technical failures, hacking and bankruptcy.

The proponents of Information-Centric networking suggest that the new technology could remedy some or all of these problems.

2.3 Information-Centric Networking

Information-Centric Networking (originally known as Content-Centric Networking) replaces the *source-based packaging* model, which forms the basis of the current Internet, with a *content-centric* model. In this model, every item of information (e.g. a scientific paper, a book, a song) has a statistically unique name. Thus information consumers who want to access a specific item of information no longer search for the *host* where the data is stored but for *named data items* - the fundamental units of transaction at every layer of the protocol stack. At the lowest layer, ICN has no notion of a host; packets address content not location.

The new architecture nonetheless preserves the design decisions that made IP simple, robust and scalable [2]. According to Van Jacobson (ibid), “much of IP’s success is due to the simplicity of its network layer (the IP packet - the thin ‘waist’ of the stack) and the weak

demands it makes on layer 2, namely: stateless, unreliable, unordered, best-effort delivery". ICN maintains these characteristics. For a detailed description of the network architecture readers are referred to Van Jacobson's original paper. Here we will focus on specific aspects of the architecture with a large potential impact.

1. *Security and ownership.* ICN's shift of focus, from hosts to content (named data) enables "content-centric security". In van Jacobson's proposal

   "Protection and trust travel with the content itself, rather than being a property of the connections over which it travels. In CCN, all content is authenticated with digital signatures, and private content is protected with encryption. (...)" [2]

   This implies, implicitly, that named data packages have an owner. It also implies that private information cannot be decrypted – that is used – without the permission of the owner.

2. *Scope.* Named data packages can be associated with a "scope" [8]. This facilitates querying and allows nodes on the network to implement specific policies for data packages with a given scope.
3. *Caching.* The use of named data packets allows intermediate nodes to cache data. In-network caching has the potential to significantly reduce the volume of traffic crossing the network, while simultaneously freeing operators from proprietary CDN solutions. The use of in-network caching also allows small or temporary information providers to provide high quality media services without large investments in network infrastructure.
4. *Network robustness.* In ICN, named data (or pointers to named data) are distributed redundantly across the network. This architecture helps to balance network traffic and eliminates single points of failure (large Internet hubs).

2.4 CONVERGENCE

The CONVERGENCE framework extends ICN with additional features, many adopted from or contributed to the MPEG community and the MPEG-21 standard.

- CONVERGENCE defines a standard data unit (the Versatile Digital Item or VDI). The CONVERGENCE middleware (CoMid) defines a standard set of operations over VDIs.
- The middleware allows users to delete a VDI, or update its content after it has been published. VDIs can also be associated with an "expiry date". This means that in principle, owners can control over VDIs for their whole lifecycle.
- Owners can monitor the way VDIs are used – defining reports, which they receive every time the system detects a particular type of event (e.g. when a user downloads or "plays" the VDI).

- The content of named data items (VDIs) is packaged with user-defined metadata. Metadata can help users (and search engines) to filter data (e.g. filtering out all media that do not meet certain technical characteristics, or all commercial offers above a given price threshold). They can also facilitate use of the data at the point of consumption (e.g. by providing technical data for media, citation data for scientific papers, provenance data for experimental datasets).
- VDIs can be associated with a license expressed in the CONVERGENCE Rights Expression Language (REL). The license determines who can see and access the VDI on what terms, and for what purposes. The existence of a license bundled with the data allows owners and users to ascertain when a user is in breach of the license. Some (but not all) license provisions (e.g. access control) are automatically enforced by the CONVERGENCE middleware.
- Like conventional ICN, CONVERGENCE comes with a content-centric model of security. However, CONVERGENCE also provides explicitly support for pseudonymous and anonymous access.
- CONVERGENCE can run over its own network layer (CoNET) but also over conventional IP.

In summary, CONVERGENCE extends the standard features provided by ICN with metadata, and with a strong concept of VDI ownership, and owner-control. One of its most important features is that its deployment does not strictly require a revolution at the network level, even if CONVERGENCE proposes its own solution for the network level itself.

3 Social and economic impact of ICN and CONVERGENCE

3.1 Tussles

The literature on the economic and social impact of ICN is sparse. A Google Scholar search for "Information Centric Networking" and "economic impact" turned up just ten papers. Searching for "Content Centric Networking" and "economic impact" produced another ten. Replacing "economic impact" with "social impact" and repeating the search we found just four additional papers.

Possibly the most interesting analyses to be produced so far are those contained in two papers by Dirk Trossen and colleagues [8, 9]. In these papers, the authors analyse the possible impact of ICN on conflicts between different social and business actors. They refer to these examples as "tussles"[1], a term they borrow from [10]

In [8] the authors make the somewhat opaque claim that ICN can improve "the delineation of tussles along well-defined boundaries" in the network architecture. In [9] they make this notion more precise, identifying categories of tussle that ICN is likely to affect. These include tussles about

- What content we want and what we get
- What we need to expose in order to get what we want
- Who owns the "user experience"
- Optimizing delivery networks
- Interconnecting networks

In this study we will focus on large-scale impacts that go beyond the telecommunications industry. Therefore, we will focus on the first three of these tussles and add two others, which we believe are of great social and economic importance.

- Who can provide commercial and non commercial content to other users
- Who can monitor and or control the information that users provide to other users

Provision and filtering of content is logically prior to consumption. It is with these "tussles", therefore, that we will begin our analysis.

[1] Tussle : ***a.*** *A vigorous or disorderly conflict; a severe struggle, a hard contest; a scuffle* ***b.*** *in figurative sense: esp. a sharp and determined contention or dispute (Oxford English Dictionary 2nd Edition)*

3.2 Who can provide commercial and non commercial content to other users

3.2.1 The Internet today

The first, revolutionary, effect of the World Wide Web was to make it possible for any organization, however small, to become an Information Provider and to enormously increase the range of information available to Information Consumers. The benefits are well recognized. Small businesses have found completely new ways of advertising and selling their goods; Information Consumers have access to more, better quality information than ever before; in many areas of the economy (telecoms, scientific publishing, music publishing, cinema, travel), the Internet has broken down barriers to market entry, drastically improving affordable access to information and reducing prices.

For the first twenty years of the World Wide Web's history, these developments were widely seen as drivers of productivity and economic growth. However, recent years have seen the emergence of critical voices. Current source-centric Internet technology provides no technical mechanism allowing information providers to unambiguously assert ownership over their products. This means that users – sometimes individuals but also large companies – can use information other users have produced without offering any form of compensation. In the creative industries (e.g. journalism, photography, education, music, film), apparently "free" offerings by Internet-based based companies have made it difficult or impossible for small businesses and individuals to earn money from their own works. This trend has deep social and economic consequences. As convincingly argued by Jaron Lanier [11], the new web economy works on the principle of winner-takes-all: a tiny group of top-tier information providers (Google, Facebook, Amazon, Apple, etc.) have grown at the expense of small businesses and individuals who have found it harder and harder to make a living. Lanier sees these trends as a mortal threat to middle-class prosperity and to the long-run future of the USA as a democratic capitalist society. Many of his arguments could be applied just as easily to Europe.

3.2.2 ICN and CONVERGENCE

As we have already seen, one of the essential concepts in Van Jacobson's proposal for ICN is content-based security: all content is digitally signed; private content is encrypted. This implies a concept of ownership. The person who signs or encrypts a piece of content is, at least in one sense, the effective owner of the content. Compared to the current Internet, in which content is represented by anonymous streams of bits, this is a major innovation.

CONVERGENCE, and the CONVERGENCE licensing concept, makes ownership over content explicit. Every VDI is associated with a license that defines who can use the content,

and for what purposes. If the owner so desires, she can define the license in such a way that she keeps the right to update or delete the VDI. She can also fix an expiry date after which all copies of the VDI will be automatically deleted from the network ("digital forgetting") and monitor the way the VDI is used. Importantly, this is true, not only for VDIs produced by major companies but also for VDIs produced by small businesses and individuals. In social, economic and political terms the shift from weak to strong owner control is a major one.

In democratic societies, the ability of an information provider to offer content to information consumers is constrained not so much by legal restrictions as by economics. Publishing information is only possible if publishing is affordable. This means that providers need to be paid for their work. The licensing mechanisms incorporated in VDIs would make this easier. Large media companies could use VDIs to monitor and control the digital films, music and books they sell – making it easier to identify illegal copies sent across the network or posted on video-sharing sites. Smaller companies and individual artists (e.g. photographers) could use VDIs to ensure they are paid when their products are used by newspapers and broadcasting stations. VDIs could also be used as the basis for new business models.

For instance a Performing Rights Society or other organization could measure how often specific VDIs are downloaded or played, allowing organizations that offer flat rate services to compensate owners in proportion to real popularity of their works.[2] Lanier [11] has even made the utopian suggestion that everyone who contributes content to an information provider (e.g. the owners of sites indexed by Google, users posting to Facebook, photographers uploading photos to Flickr) should receive a share of the provider's overall revenue. VDIs would provide an ideal mechanism for implementing this kind of proposal. According to Lanier, the result would be a shift towards an economy with a more equal distribution of wealth and opportunity than is currently the case. Such a shift might command support from a broad spectrum of political opinion. In his view, it might also be the only way of guaranteeing the long-term sustainability of Western capitalism.

We will postpone discussions of likelihood until the end of this paper. First, however, we observe that ICN and CONVERGENCE will not only affect who can publish information. It will also affect who can monitor and control information and what information, in the end, we will be able to consume.

[2] At the time of writing companies like *Spotify* sign licensing agreements that allow the company to freely distribute a certain package of content in return for royalty payments to the owner of the material. This arrangement is presumably good for both parties. However, it is not effective as a way of compensating independent artists who have not « signed » with a major media company.

3.3 Who can monitor and or control the information that users provide to other users

3.3.1 The Internet today

In its early years, the Internet was celebrated for its freedom from government control. When John Gilmore stated that "The Internet treats censorship as though it were a malfunction and routes around it" (cited in [12]), he was widely believed. Even today, the “free Internet” is credited with a major role in the Arab spring [13, 14] and in the gradual opening of China [15]. However recent years have also seen the emergence of more worrying tendencies.

First, the dominance of the Internet by a tiny number of very large companies has changed the way information is monitored and controlled. At the most visible and possibly the most benign level, Google, Facebook, Apple and Amazon filter the information they make available to their users, making it difficult for information providers to distribute information, that contravene their “terms of use”, or that are alleged to do so. As private companies, some prevent providers from distributing materials (e.g. adult and some political content) that in most Western jurisdictions would count as constitutionally protected speech.

A second, probably more serious problem is that large information brokers provide an easy target for government censorship and private litigation, both of which are expanding rapidly. Google [16] for example, regularly complies with requests to “take down” information that is illegal in a particular jurisdiction (e.g. holocaust denial in France, *lèse majesté* in Thailand, criticism of public officials in many different countries) or that is claimed to be defamatory. Domination of the Internet economy by a very small number of companies facilitates the task of the censors. In the meantime, governments are improving their ability to control the Internet directly. Many observers were shocked at the ease with which the Egyptian government “ switched off” the Internet during the revolution of 2011 [13] but in fact this act was only an example of a broader trend. For many years, for instance, the Chinese “great firewall” has succeeded in limiting – without blocking - Chinese citizens’ access to foreign Internet sites [17]. More recently many governments have deployed deep package inspection technologies to identify and close down encrypted channels of communication (Skype [18], TOR [19], VPNs [20]) that political dissidents frequently use in their communications.

A third issue is that all large Internet services systematically collect information about the behaviour of their users, which they use to “personalize” their services and to sell targeted advertising. This practice provides large Internet companies with an enormous competitive edge over companies with less effective access to customer information. Other effects are more subtle. In particular, users who repeatedly access a specific class of information (e.g. “conservative-learning news”, “liberal-leaning news”) automatically receive more and more of the information they like and less and less of other kinds of information. Several authors

have suggested that automated matching of information to user preferences by a very small number of news sources, increases political polarization and decreases citizens' ability to engage in constructive dialog with citizens with different backgrounds and opinions [21, 22].

It should also not be forgotten that many Internet services (e.g. Google, Facebook, specialized services that assemble information on individuals from public sources) provide a powerful tool for private monitoring and surveillance (e.g. monitoring of employees by employers, monitoring of children by parents, surveillance within personal relationships etc.).

3.3.2 ICN and CONVERGENCE

As mentioned earlier, one of the most important aspects of ICN is content-centric security. CONVERGENCE reinforces this security with licenses and enforcement mechanisms designed to ensure that VDIs are only visible to their intended users.

It is possible that these mechanisms can prevent some forms of web surveillance. For instance, posters could license "posts" to social network sites in such a way as to exclude anyone except their friends from reading the posts. At least potentially the license could also exclude Facebook administrators. More radically, ICN and CONVERGENCE mechanisms would provide a possible mechanism for distributed implementations of social networking with no central mediator, such as those proposed by the Diaspora project [23]. Similar techniques could be used to implement secure access control for web sites and blogs. If web pages were implemented in the form of VDIs, access could be restricted to particular users or groups of users; CONVERGENCE-compliant search engines could index web sites but only show search results and serve up pages to duly authorized users. This kind of protection could limit private and government surveillance based on direct access to the content of posts, web pages etc.

However, other applications of ICN and CONVERGENCE may be less benign. One of the key features of ICN content-centric security is that all content is digitally signed and authenticated as it traverses the network. If this measure were universally implemented media companies could use the technology to identify users who "share" the content to which they claim ownership. Retailers could use it to identify and monitor their customers. Perhaps most significantly governments could use it to identify links between Information Providers and Information Consumers, posing a threat to the use of the Internet by political dissenters or whistle blowers. Many citizens will see some or all of these practices as a threat to their freedom.

CONVERGENCE provides mechanisms for pseudonymous and anonymous access to ICN. However, pseudonymity is no defence for users engaged in what some governments may regard as illegal activity (e.g. organization of political demonstrations or strikes, file sharing)

and even anonymity could be a double-edged weapon: in a system in which most users certify their identity, use of an anonymous ID would signal a user for special attention.

A second aspect of CONVERGENCE with potentially negative effects is the use of user-defined metadata to describe VDIs. If the technology is to fulfil its full potential (e.g. facilitating search) metadata should provide an accurate description of the content of the VDI. However, accurate metadata also facilitates tracking of content by government and commercial operators. Users could thus be induced to package "sensitive" content with false metadata. If such practices spread they would obviously reduce the value of the new technology.

3.4 Consuming information: what information we want and what we get

3.4.1 The Internet today

The modern Internet gives Information Consumers access to a broader range of information sources than at any time in history, including not only content from professional Information Providers but also vast volumes of user-generated content (Wikipedia, blogs, Facebook posts, youTube posts, Flickr photographs etc.), some of extremely high quality. In many different sectors of the economy (e.g. scientific publishing, medical information) new business models enabled by the Internet have enormously improved public access to valuable content, particularly in the developing world. For instance, the Internet has made it possible for African farmers to access information on market trends, that can help them to plan their production [24, 25]. Meanwhile, the diversity of the information on offer has allowed huge numbers of users to broaden the cultural, political and personal horizons. These are important advances.

This does not mean, however, that the Internet is an information utopia. There is strong evidence that even professional users of the Internet often rely on a limited set of information sources [26, 27]. This implies that users' access to information depends on the policies adopted by a small number of large private companies, who have the means to filter out information that is not consistent with their marketing policies (e.g. adult, religious or political content) or their political preferences[3]. This is a disturbing development. It has also been observed that current patterns of Internet use encourage "confirmatory bias" – the tendency of Information Consumers to choose sources of information that confirm rather than question their existing opinions [21].

[3] At the time of writing, there is no evidence that search companies are biasing search results to favour their own political agendas. This remains nonetheless a strong theoretical possibility.

Other problems concern the degree of knowledge required to use current tools. Nowhere is the digital divide so apparent as in the differing abilities of information "haves" and "have-nots" when searching for information or when trying to distinguish reliable from unreliable sources of information [28, 29].

3.4.2 ICN and CONVERGENCE

Good implementations of ICN and CONVERGENCE technology could make information search significantly easier – especially when search involves structured information contained in VDI metadata. It is also worth noting, however, that "semantic web" technology has been offering these possibilities for many years, with relatively little impact on mainstream applications. A degree of scepticism is therefore in order.

CONVERGENCE and ICN could also help to reduce information overload by helping users to filter irrelevant content. This possibility would be especially powerful if it were combined with regulations obliging providers to label kinds of content many users seek to avoid (e.g. ads, adult content, political broadcasts, soap operas etc.). It could also make it easier for content providers to provide users with material that matches their preferences, ascertained through analysis of their previous transactions.

Perhaps, more significantly, at least in the long term, strong owner control over content could make it easier for professional producers of content to earn their living – thus improving the quality of the information available over the Internet.

However, these advantages would not necessarily be cost-free. In particular, the introduction of technologies allowing strong owner control over content could reduce the availability of content for users who are unwilling or unable to pay for it. It is easy to foresee scenarios in which large information providers would use the technology not just to limit consumer access to free films, and music, but to restrict unpaid access to books, newspapers and medical journals. Particularly in developing countries, such restrictions could be extremely damaging.

Ease of information filtering could also prove a mixed blessing. While accurate metadata would undoubtedly make it easier for users to filter out unwanted content, it would also facilitate filtering by search engines, ISPs, cloud providers, apps stores, and telecoms operators. Even without government regulation, commercial pressures could lead to restrictions on content which particular commercial actors found undesirable (e.g. sex education, textbooks on biological evolution, creationist tracts, religious propaganda). In many countries, government regulation of particular kinds of speech, implemented through network providers, would add additional limitations.

Finally, as mentioned earlier, ICN and CONVERGENCE would make it easier for large Information Providers to filter out information that does not match consumer preferences. Although this would reduce information overload for consumers, it would also reduce the

frequency with which consumers "chance" on information that challenges their existing opinions and beliefs. This would not necessarily be a good thing.

3.5 What you have to give up to consume the information

3.5.1 The Internet today

In the modern Internet economy, mega-sites such as Facebook, youTube, Flickr depend exclusively on data uploaded by users, while others (e.g. Google) base their success on the content of third party web sites. In theory, users can refuse to use the services and web sites can block access to Google robots. However, in practice, most individual and institutional users are unwilling to accept the social and economic costs of "going off-line". In other words, social and economic pressure forces users to provide content and information without receiving any compensation for their services.

Additionally, all large sites collect information about the behaviour and preferences of their users or use commercial services to collect the data on their behalf. In both cases, they use the data, not just to personalize the content they provide to users, but as the basis for targeted advertising. In the case of Google, this ability, combined with Google's huge audience, has turned the company into the world's most valuable online advertising agency [30].

In summary, the free services these sites offer their customers and their ultimate profitability depend on users providing them with free content and information. In sites requiring a login, this "bargain" is enshrined in the terms and conditions the user accepts when she registers with the site.

3.5.2 ICN and CONVERGENCE

If widely adopted (see the discussion in section 4), ICN and CONVERGENCE have the potential to change the nature of the relationship between large Internet sites, smaller professional information providers and individual users.

1. CONVERGENCE licensing and tracking technology, combined with content-centric security, would allow professional information providers (e.g. newspapers) to charge third party services for the use of their content.
2. At least in theory, the same technology could also be extended to individual users, supporting Lanier's proposal [11] that they should receive micropayments every time a site uses their content.
3. CONVERGENCE-supported pseudonymous ID's would allow users to access sites without revealing their individual identities, preventing sites from tracking their

personal behaviour and preferences and thus from selling targeted advertising[4]. In other words, use of pseudonymous ID's would create financial losses for advertising-centric companies. Companies could avoid these losses only by paying users to use traceable IDs issued by the company.

4. If existing Internet companies were not willing to pay for content and personal information, ICN and CONVERGENCE would create opportunities for new companies offering *rendezvous* services (services matching user *subscriptions* to data items – or VDIs – published on the network) and CONVERGENCE-based social networking.[5]

In summary, ICN and CONVERGENCE have the potential to reduce the unpaid transfer of content and personal information from individual users to third party web services. Such a change could potentially change the shape of the Internet economy. Obviously, however, this depends on whether or not the changes are actually implemented. We will discuss this issue in the next chapter.

3.6 Who owns the user experience?

3.6.1 The Internet

Another set of "tussles" identified by [9] are tussles about "who owns the user experience". Even though the expression is somewhat obscure, the conflict Trossen identifies is real: what is at stake is who monetizes the content users see on their screens.

In the period before the World Wide Web and in the years immediately after its introduction, many medium-large companies (CompuServe, America Online, large telecommunications operators, smaller ISPs) created "closed" information services that did not directly link to third party content, or which depended only partially on this content. The services were profitable for a period, but as users discovered the wealth of information directly available through the web, they failed.

In the last ten years closed information services have been largely replaced by new services that depend on information "scraped" from the web (Google, Bing) or on User Generated Content (Facebook, Flickr, youTube etc.). Unlike their predecessors, the companies that run these services do not offer network services and do not charge for access.

[4] In this scenario, pseudonymous and individual IDs would be mathematically indistinguishable, preventing companies from discriminating against "untrackable" users.

[5] An ICN/CONVERGENCE-based social network would not need a central server and could be advertising free. Alice publishes posts to a set of friends, using the REL to define the conditions under which they can relay the posts to other users. Bob subscribes to posts by Alice and his other friends, using CONVERGENCE metadata to whitelist and blacklist specific classes of information. Content-centric security combined with digital forgetting would reduce privacy risks. This is very similar to the scenario proposed by the recent Diaspora Project.

This development has had a negative impact on telecommunications operators and ISPs who carry the traffic generated by the new operators and bear the costs, but who have little or no ability to monetize the "customer experience" and who have lost brand visibility. In the face of rapidly increasing network traffic, operators have been forced to invest in Content Delivery Networks, to reduce operating costs. Attempts to charge major services for delivering their content have been unsuccessful.

In recent years, many content providers, particularly newspapers, have begun to shift their content from free web sites to proprietary apps, often running on multiple platforms. To the extent that this move is successful it is shifting "ownership of the user experience" back to the Information Providers and providing them with new revenues. The risk, as pointed out by many observers, is a return to closed information systems, lacking the richness and diversity of the best of the web.

3.6.2 ICN and CONVERGENCE

If broadly adopted ICN and CONVERGENCE would increase owner control over content. Such a development would strengthen Information Providers' ability to generate revenue and weaken the role of the major services that dominate today's Internet economy - a major power shift. Interestingly the key players would be Information Providers (especially large ones) and today's large services – not Telecoms operators. It is hard to imagine scenarios in which operators could recover the ground they have lost.

4 Futures, probabilities and the public good

4.1 Obstacles to the introduction of ICN and CONVERGENCE technology

A realistic assessment of prospects for ICN and CONVERGENCE must recognize the huge technical and political obstacles facing the new technologies.

1. In technical terms, adoption of ICN at the networking level would require the installation of new software on routers throughout the world. The slow uptake of IP v6 suggests that this would be, at best, an extremely slow process.
2. In political and economic terms, the current architecture of the network offers real and perceived benefits to a huge range of actors including large Internet companies such as Google and Facebook, anonymous consumers who enjoy access to free services and political dissidents who value the relative anonymity of the current architecture. If these actors were to choose freely they would almost certainly choose business as usual. They could also exert significant political pressure in defence of the current system.
3. In the current Internet economy, the actors with the strongest interest in promoting the new architecture (small and medium-sized information providers) are economically and politically weak. It is not easy to believe that they could mount a successful challenge to current power relationships and technical architectures.
4. The trend towards "business as usual" would be accentuated by consumers' normal reluctance to adopt any new technology without a compelling reason.
5. The value of the new technology to users would depend on so-called network effects [31], that is on the number of users who adopted it. If the number of early adopters were low it would initially have very little value. In these conditions massive adoption seems very unlikely.

4.2 Factors favourable to ICN and CONVERGENCE

Despite the apparent solidity of the current Internet economy, a number of factors are making it increasingly fragile.

1. Public and government awareness of the economic power of very large Internet companies is growing. The current debate focuses on tax avoidance and on the negative effects on specific industries (retailing, newspapers, the creative industries). In some countries it is leading to legislation, and judicial decisions restricting the ability of these companies to exploit third party content without compensation. One example is proposed German legislation forcing search engines to pay to index German newspapers [32].

2. Another cause of fragility is increasing public sensitivity (in Europe but also in the United States) to issues of personal privacy and the use of personal information for commercial purposes. This has the potential to lead both to regulatory changes, and to a shift of consumers away from services that not offer sufficient privacy guarantees.
3. All the large Internet companies distribute their computing and communications resources across multiple physical sites and have a good record for continuity of operation. Inevitably, however, dependency on a small number of very large companies decreases the robustness of a network architecture that was originally designed to survive nuclear war.

Because of these risk factors, the current Internet economy is vulnerable to unpredictable political, military, economic and technical events. A non-exhaustive list of examples might include: widespread adoption of new taxation or privacy regulation that damage existing business models; major scandals involving illegal use of personal data for political or commercial purposes; successful cyber-attacks against a major player, with long interruptions in service and/or loss of user data; bankruptcy of one or more major companies; contagious loss of customer satisfaction with existing services.

Any of these events could make novel technologies and business models more attractive to consumers, creating new opportunities for ICN and CONVERGENCE. It is even conceivable, though not likely, that they could lead to solutions similar to those suggested by Lanier [11] in which individual and corporate users systematically use ICN and CONVERGENCE technology to assert ownership over their personal information and to charge third party services for using the information.

Perhaps more realistically, it is not difficult to imagine "niche applications" in which Information Consumers and Information Providers would both benefit from the new functionality provided by ICN and CONVERGENCE. These might include

- *B2B scenarios* in which professional Information Providers sell content to professional Information Consumers (e.g. newspapers and magazines) who need to be certain of the provenance of the content they purchase, and who do not want this content to escape into the public domain.
- *Medical scenarios* in which medical professionals (e.g. primary care physicians and the doctors treating a patient in an acute medical emergency) share confidential patient data.
- *Publishing scenarios* in which individual authors and publishers make their works available to the public, either directly or through public services such as the Digital Public Library of America [33, 34] while simultaneously using CONVERGENCE licensing to assert ownership.

- *Social networking scenarios* in which software developers use CONVERGENCE technology and ICN to create distributed social networking solutions that allow users to share personal information in a secure way without relying on a centralized service.

CONVERGENCE middleware, unlike a fully-fledged ICN solution, can run over a conventional IP stack. Therefore, the adoption of CONVERGENCE or similar technologies to support the requirements of specific scenarios would not require an improbable redesign of the Internet. The availability of standards and middleware would facilitate such implementations.

The size of the Internet, the weight of existing investment and the enormous economic and political interests vested in the current Internet architecture make rapid, wholesale change extremely unlikely. But they in no way prevent the creation of islands of innovation, in which new technologies can be perfected and deployed at relatively low cost. This is possibly the most plausible scenario for the spread of ICN, CONVERGENCE, and other technologies offering radical innovations in the capabilities of the Internet.

4.3 The public good

We have argued that ICN and CONVERGENCE, if widely adopted, could strengthen the economic and political role of Information Providers with respect to the large centralized services that dominate the current Internet economy. At least in theory, the change could extend from large corporate providers of information (e.g. newspapers) to the individual users who feed services like Facebook, Instagram and Flickr.

Such a broad shift could have a positive impact on the ability of Information Providers to earn a living from their work and on the quality and quantity of information available to end-users. But it could also reduce access to information for countries and individuals who cannot afford to pay for it, and reduce the diversity of views available to users. It could make it harder for web sites to collect information that users wish to keep private and support digital forgetting but it could also make it harder for political dissidents to maintain their anonymity on the network. In brief, the new technology has the potential to affect multiple dimensions of economic social and political life, with different effects on different actors. Whether the net effect on the public good would be positive or negative is impossible to predict.

CONVERGENCE– like other research projects – has created new “possibles” – building blocks for future development. How they will be used is and must be an open question.

References

1. Jacobson, V., et al., *Content-centric networking.* Whitepaper, Palo Alto Research Center, 2007: p. 2-4.
2. Jacobson, V., et al. *Networking named content*. in *Proceedings of the 5th international conference on Emerging networking experiments and technologies*. 2009. ACM.
3. Taleb, N.N., *The Black Swan: The Impact of the Highly Improbable*, 2007, New York: Random House.
4. Taleb, N.N., *Anti-Fragile*, 2012, London: Allen Lane.
5. Kauffman, S., *Reinventing the sacred*, 2008, New York: Basic Books.
6. Garey, M.R. and D.S. Johnson, *Computers and intractability: a giude to the theory of NP-Completeness*, 1979: Bell Telephone Laboratories.
7. Ericsson, A., *Business Dynamics of the Future Networks.* 2011.
8. Trossen, D., M. Sarela, and K. Sollins, *Arguments for an information-centric internetworking architecture.* ACM SIGCOMM Computer Communication Review, 2010. **40**(2): p. 26-33.
9. Trossen, D. and A. Kostopoulos. *Exploring the tussle space for information-centric networking*. 2011. TPRC.
10. Clark, D.D., et al. *Tussle in cyberspace: defining tomorrow's internet.* in *ACM SIGCOMM Computer Communication Review*. 2002. ACM.
11. Lanier, J., *Who owns the future?*, 2013, London: Allen Lane.
12. Barlow, J.P. and J. Gilmore, *Illustration Censorship 2000.*
13. Allagui, I. and J. Kuebler, *The Arab spring and the role of ICTs: editorial introduction.* International Journal of Communication, 2011. **5**(2011): p. 1435-1442.
14. Stepanova, E., *The role of information communication technologies in the "Arab Spring"*. PONARS Eurasia, 2011(15): p. 1-6.
15. Chi, E., *The Chinese Government's Responses to Use of the Internet.* Asian Perspective, 2012. **36**(3): p. 387-409.
16. Google. *Google Transparency Report*. 2013 April 1, 2013]; Available from: http://www.google.com/transparencyreport/removals/government/.
17. King, G., J. Pan, and M. Roberts. *How censorship in China allows government criticism but silences collective expression*. in *APSA 2012 Annual Meeting Paper*. 2012.
18. Deibert, R., *Access denied: The practice and policy of global internet filtering*, 2008: MIT Press.
19. Winter, P. and S. Lindskog. *How the Great Firewall of China is Blocking Tor*. in *Proceedings of the 2nd USENIX Workshop on Free and Open Communications on the Internet*. 2012.
20. Eissa, T. and G.-h. Cho, *Internet Anonymity in Syria, Challenges and Solution*, in *IT Convergence and Security 2012*2013, Springer. p. 177-186.
21. Knobloch-Westerwick, S. and S.B. Kleinman, *Preelection Selective Exposure Confirmation Bias Versus Informational Utility.* Communication Research, 2012. **39**(2): p. 170-193.

22. Iyengar, S. and K.S. Hahn, *Red media, blue media: Evidence of ideological selectivity in media use.* Journal of Communication, 2009. **59**(1): p. 19-39.
23. The Diaspora Project. *The Diaspora Project*. 2013 [cited 2013 April 13]; Available from: http://diasporaproject.org/.
24. de Boer, V., et al. *RadioMarch: distributed voice-and web-interfaced market information systems under rural conditions*. in *Advanced Information Systems Engineering*. 2012. Springer.
25. Henriques, J.J. and B.E. Kock. *Empowering Smallholders and Local Food Markets with Smartphones and Social Networks*. in *Global Humanitarian Technology Conference (GHTC), 2012 IEEE*. 2012. IEEE.
26. Arroll, B., et al., *The Overview*.
27. Grayson, L. and A. Gomersall, *A difficult business: finding the evidence for social science reviews.* London: ESRC UK Centre for Evidence Based Policy and Practice, Queen Mary University of London, 2003.
28. Jean, B.S., et al., *An analysis of the information behaviors, goals, and intentions of frequent Internet users: Findings from online activity diaries.* First Monday, 2012. **17**(2-6).
29. Hargittai, E. and H. Young, *Searching for a Plan B: Young Adults' Strategies for Finding Information about Emergency Contraception Online.* Policy & Internet, 2012. **4**(2): p. 1-23.
30. Moon, Y. and D. Chen, *Google Advertising*, 2007: Harvard Business School Publishing.
31. Gilder, G., *Metcalf's law and legacy.* Forbes ASAP, 1993. **27**.
32. Williams, C., *Google battles German newspapers over charging*, in *The Telegraph*2012: London.
33. Darnton, R., *The national digital public library is launched.* New York Review of Books, 2013(April 25, 2013 (advanced e-publication)).
34. DPLA. *Digital Public Library of America - Home Page*. 2013 [cited 2013 April 13]; Available from: http://dp.la/.