Two of the Grand Changes through Computer and Network Technology

Bart Jacobs

Two of the Grand Changes through Computer and Network Technology

Bart Jacobs

Institute for Computing and Information Sciences, Radboud University Nijmegen
P.O. Box 9010, 6500 GL Nijmegen, The Netherlands.
Email: bart@cs.ru.nl URL: http://www.cs.ru.nl/~bart

Abstract. This essay identifies and discusses two grand changes that are part of the widespread use of computer and network technology, namely (1) the separation of content and carrier, and (2) the transition from broadcast to point-to-point communication.

Although it is all too easy to think that we are living in revolutionary times, it is fair to say that computer and network technology has had a profound influence on our individual lives and on society as a whole. This influence is of a global scale. My aim in this essay is to elicit some essential features of these changes. I'm not content to just observe that computer chips and systems have become smaller, faster, and more connected, but I wish to explore some of the more fundamental "grand" changes that come with the widespread use of computer technology. Thus, I'm looking for big, possibly even paradigmatic, changes instead of incremental ones.

Two such grand changes are identified, namely:

1. the separation of content and carrier;
2. the change from broadcast to point-to-point communication.

This essay contains a discussion of these two changes and their consequences.

The work presented here is not based on empirical research. Instead, it is based on my own analysis of the developments, on discussions with colleagues, and on the literature. In the end it is difficult to say whether the analysis presented here is "true" or "false". But hopefully it does help to clarify and see some structure in the developments of the past few decades. My aim is to present the developments neutrally, in a non-judgemental manner, but I am well aware of the difficulty, or even impossibility, of doing so, since many issues are highly political. Therefore, in the end, it is better to see this article as a personal essay, and not as a solid scientific study.

This essay consists of two parts, each of which first describes the relevant grand change, and then discusses some of its consequences.

1 The separation of content and carrier

When you buy a book, you get at the same time both the *carrier*, namely the book's paper pages bound together, and the *content*, namely the book's

text. This unity of content and carrier has been the norm for centuries, also in other fields: a painting consists both of a carrier, namely the painted cloth, and content, namely the image; an LP record consists of a vinyl disc, as carrier, in which music, as content, is encoded in its grooves.

The emergence of digital media formats has separated content and carrier. This separation has many consequences, as are discussed below. It happened roughly in the 1980s and 1990s. For the generations that grew up after 1980 it is strange that you have to pay for the pages of a book, or for a CD: it is much easier — and cheaper, in principle — to get the content without the carrier. The carrier has almost become an anomaly.

True, content still needs some form of carrier, like a hard disk, a USB stick, or even a DVD. Content can even be stored somewhere in "the cloud", where the carrier itself is completely invisible to the user. An important aspect of digital content is that it can easily be copied or transferred from one carrier to another, without loss of quality. Also, the direct costs of such a transfer are usually zero, given that most people have flat rate connections. At most, the copying takes some time. In contrast, copying in earlier days, when carrier and content were still united, resulted in small changes of the content, either in form, message, or quality.

Before looking into the consequences of the lost unity of content and carrier, I would like to address three finer points. First, one may argue that the separation of content and carrier started with the introduction of tape recorders and audio cassette players. They involved analogue audio recording. Copying, from one tape to another, meant significant loss of quality, notably through the increase of noise. Hence there was still some bond between the original carrier and the content. These tape recordings are thus not the clearest example of the change that I am trying to identify; they are a precursor.

Second, one may argue that "copying without loss of quality" is the more important change, more fundamental than "separation of content and carrier". The two are of course closely related. Still, copying without any sign of loss seems the more instrumental aspect, whereas the content-carrier separation is of a more conceptual, maybe even paradigmatic, nature.

Third, this discussion about carrier and content bears some resemblance to the discussion about atoms and bits, as initiated in [5]. However, the focus there is more narrow and concentrates on commercial value.

Controlling information carriers

A basic consequence of the lost unity of content and carrier is that one can no longer control the spread of information by controlling the spread of the carrier. Since a carrier is a tangible, physical substrate, its movements can be monitored and controlled via traditional searches and confiscation. This is a hard lesson, primarily for oppressive authorities, but also for individuals who wish to keep their information private. As we shall see, the lost physical control has now been replaced by new forms of control in the digital world.

Historically one can find many examples where authorities tried to control the flow of information via the information-carriers. One can think of the right to publish books, explicitly granted only to Cambridge University, in 1534 by Henry VIII of England. In the 17th century Holland became Europe's main book publisher because of its free climate, without much censorship. These examples address (non)interference with the production/sending of information. But also the consumption/receiving of information could be controlled in the past via the information-carriers. The Vatican long used its *Index* for blacklisting unwelcome books, and the book-burnings of the Nazis in the 1930s were public actions against subversive literature. These days such carrier-control mechanisms no longer work and are completely ineffective. For instance, the British Government was ridiculed in July 2013 when it ordered the Guardian newspaper to destroy a few hard drives with information leaked by Edward Snowden. The sensitive information had long been copied to several other carriers, located elsewhere.

Democratic governments have become more relaxed about citizens' access to information, except in cases where their own secrets are involved, like in the Bradley Manning (wikileaks) or Snowden examples, or where the content is clearly illegal, like in child pornography. Modern constitutions have "free press" clauses, guaranteeing the freedom to publish. In the past such publishing involved "physical" aspects, related to the carrier (books, newspapers, radio/TV signals) that required certain investments and physical infrastructure. Today everyone can be a publisher, via blogs, tweets, comments, webpages, *etc.* because information is separate from a fixed carrier and can be copied and spread easily. Thus, freedom to *send* information has become easy and is often take for granted. Freedom to *receive* information is becoming an issue, as is discussed towards the end.

Beyond controlling carriers

The reaction to the carrier-content separation is different in the public and private sector. These differences are described briefly.

The private sector has tried various technical copy control measures to restrict the consumption of digital information, under the name 'Digital Rights Management', commonly abbreviated as DRM. These approaches focus on the users' devices, in particular on the way of organising and accessing data at these endpoints. The movie and music industry — often referred to as the content industry — has been a strong proponent of DRM techniques. DRM restrictions may apply to the copying itself, or to the viewing or listening process. The former often involves protective measures at the hardware level, whereas the latter involves some level of auditing on the users' side (which raises privacy concerns). Many of these DRM techniques have been broken and turned out to be less successful than expected. DRM has not disappeared completely, but survives often in lightweight form as part of a set of other control mechanisms, such as listed below.

– Locking customers into a closed hardware-software eco-system, like Apple does.

– Enforcing proprietary data or storage formats, like Microsoft does, or some game producers.
– Seducing users to put all their data in your own cloud, like Google, and many others, do.
– Building cryptographic authenticity checks into your hardware, like for printer cartridges.
– Introducing cryptographically closed domains, as in the Trusted Platform Module (TPM) approach. When added to ordinary computer hardware, TPM can assure the integrity of the platform, and thus keep content within a closed domain that is trusted by the content provider.

All these approaches are controversial because they decrease the possibilities of the users and/or increase the control by external parties, like hardware/software vendors, content owners, law enforcement, intelligence. These copy control measures have been developed almost exclusively in the private sector, in order to protect commercial interests related to exclusive access to information.

In the public sector most democratic regimes have realised by now that it is nearly impossible these days to prevent altogether that citizens receive available information. What can be done technically, *e.g.* by address filtering, is restricting access to certain services, like YouTube or Facebook. This happens from time to time in countries like Pakistan, Turkey or Iran; they do have democratic elections but at the same time rather explicit public interference with what is morally acceptable or not. Actually filtering specific content is technically much more difficult and requires rather draconian measures, like in the 'Great Firewall of China'. Its main role is to prevent destabilisation of the regime.

More democratic regimes concentrate not so much on blocking information but on getting access to the flow of information in order to keep a finger on the pulse. They have thus moved their attention from the information carriers to the channels that carry the information from one place to another. Thus they developed both technical and legal means for intercepting, and retaining data, for instance in:

– lawful interception, such as tapping mobile or landline phones or tapping internet connections. By law, communication service providers are obliged to organise their systems in such a way that they can provide all communications of individual users, upon a lawful request.
– meta-data retention, like via Europe's data retention directive from 2006, which forces telecom/internet providers to retain between 6 and 24 months who communicates with whom, where and when, but not the content of the communication. This is also called traffic analysis and is useful for relationship mapping, or for obtaining location information. Meta-data are very sensitive from a privacy perspective, because they include location information and contacts, and may for instance reveal that you have been in communication with an abortion clinic.

Increasingly this data interception is hindered by the use of advanced forms of encryption that are unbreakable by police and intelligence services. Here one sees three approaches, which may occur in combined form.

1. Making computer intrusion legal for the police, so that users' endpoint devices may be hacked and data can be accessed before (or after) encryption takes place. In many countries the intelligence services already have the legal power to intrude computers of targets. Such "endpoint operations" are currently more effective for the US National Security Agency (NSA) than breaking into the cryptographic protection of intercepted messages, see [1].
2. Obtaining access to users' data at the other endpoint, namely at the internet company, like Google or Facebook, where the data resides. This is the approach of NSA's PRISM programme. Accessing the data at such a company is of course much easier than tapping the data as it travels the internet, often via different routes, and then assembling the various packets.
3. Undermining the cryptographic techniques and implementations that are used to protect the communications going over the channels. According to recent revelations of Snowden, this approach is also actively pursued by the NSA and by the UK Government Communications Headquarters (GCHQ).

All three approaches are highly controversial because they directly affect the balance of power between the state on the one hand and private companies and citizens on the other. These approaches lead to discussions about how far police and intelligence services should go and how much collateral damage is acceptable.

Transparency

The initial hope of internet pioneers was that, once the unity of carrier and content disappeared, information would be free and could no longer be used or abused to support unequal power relations. Through the carrier-content separation it would no longer be possible to keep information locked-up in government or corporate cabinets. Such information would be freely available to all, making decision-making transparent and preventing abuse of power. How naive!

Today we see that it is not the authorities that have become transparent but rather the citizens themselves. Social media have given people the means to be seen and to share their experiences continuously. For many of us the desire to be visible is stronger than the desire to protect one's private information. Commercial companies, including in particular the social media companies, are keen to advocate such "frictionless sharing" as the right way to behave and to exploit the resulting streams of revelations for various forms of profiling and for behavioural targeting of advertisements. Public authorities can expand their own span of surveillance by demanding access to the many electronic trails that people leave behind in databases of commercial organisations.

Between 2009 and 2011 there was a similar level of naivety regarding the role of social media in the various social uprisings in the Arab world. The social media may have played a role initially in organising people to rally, but in many countries the authorities reacted quickly: by shutting off or limiting the transfer of social media messages, or by exploiting them later for their own benefit, to track and round up those that sent subversive messages, see also [3]. Social media

are not "freedom tools": they expose people, for commercial reasons, and do not offer any form of protection, especially not against oppressive regimes.

Having all data freely available is not desirable, because governments, companies, and individuals all have a vested interest in keeping certain information secret, at certain stages. This interest should be acknowledged. The German hacker organisation *Chaos Computer Club* (CCC) uses the sensible slogan *öffentliche Daten nützen, private Daten schützen*. Its message can be interpreted as: public data should be used, private data should be protected.

Business models, rewards and quality control

In economic terms, the production of digital content has high fixed costs, but low marginal costs. For instance, the production of a game or a movie requires substantial investment, but once a single specimen of the digital content exists, the cost of producing more digital copies is almost zero.

In the age when carrier and content were still united, there was an intermediate reproduction and distribution process to get the carrier, together with its content, in the hands of the different consumers. Payment happened with the transfer of carriers, in the other direction. Because these intermediaries had financial interests in the whole physical infrastructure, they tended to interfere in the production of the content, to ensure a level of quality that increased the likelihood of revenues. For instance, book publishers are picky about the authors they contract and often help authors to edit their manuscripts.

In our digital age it is often claimed that these intermediaries are no longer needed. It is true that certain sectors, like for instance the travel agency business, have changed dramatically because their role as intermediary, for instance between a traveller and an airline, is no longer needed. Some travel agencies survive in niche markets — like eco-tourism — where they can help travellers to select, and thus offer added value and quality.

Similarly, publishers of books, movies, music *etc.* need to adapt to this reality. For a long time there was a tendency to hold on to old business models, based on carriers, supported by controversial copyright laws and copy control mechanisms. Instead, the business should be based on fair rewards, primarily for the producer of the original work of art, but also for the remaining intermediaries that can offer true added value, for instance, via quality control, pre-selection, or distribution and payment of digital content. Within the sea of self-produced content without any quality control there is still a valuable role for intermediaries that focus on quality selection, and that understand their new, more modest position in the market. In fact, the value of information increases with selection, and decreases if there is an overload.

Non-tangible assets

The most profound consequence of the carrier-content separation is possibly also the most obvious one: content/information is no longer tangible. Through

the widespread use of computer technology and the ensuing digitisation, information has become very valuable, for public and private organisations, but also for individuals. At the same time these most precious digital assets are invisible and intangible, and thus hard to protect. Some crucial digital (strategy/product/personal/...) document may be stolen from you without you even noticing that the theft took place. The document can be obtained via remote access to your computer, by abusing some security vulnerability. In contrast, if the information exists only in unity with its carrier, one would either have to steal the carrier or photocopy the content. In the first case you may notice the missing carrier quickly, and in the second case you may notice the act of copying, because it requires physical proximity and time.

Our human intuitions regarding safety and security are still very much connected to the physical world. If you ask an arbitrary person in the street for his/her front-door key, you will probably hear: "go away". But if you ask people online for their login credentials, many more people reply. They don't see the value of digital information. In this sense we, as humans, have not really adjusted our values and intuitions to the new reality where content and carrier are no longer united.

2 The change from broadcast to point-to-point communication

In the area of computer networks a distinction is made between *broadcast* and *point-to-point* communication. A broadcast message is sent to everyone on the network. A point-to-point message is sent only to a specific party: the message is going from one point, the sender, to a single other point, the receiver. This means that the message should include a destination address[1].

This distinction between broadcast and point-to-point is useful in a broader context. For instance, traditionally, radio and television signals are distributed in a broadcast manner, namely by a transmitter tower that sends the signal into the ether, for everyone to receive. Locally, you select, on your own radio/TV receiver, which channel you wish to tune into. Which choice you make locally is invisible centrally, for the transmitter. But there is now also IP-based radio/television, where the signal is sent over the internet, upon request, to specific users only, identified by their IP-addresses. In that case the local choices are visible at the central server. Similarly, the distribution of news articles in a paper may be understood as 'broadcast', because every subscriber/buyer gets the whole newspaper, and decides locally which article to read. Again, these local choices are invisible in the newspaper's office. But when you read the news online, on the web, you select only those news articles that you are actually interested in, by clicking, and only those are sent to you (or more precisely: to the IP-address of your computer).

[1] There is an intermediate form in which an encrypted message is sent to everyone, but where only one or more specific parties can decrypt it. Conceptually, this is still point-to-point communication.

The following table gives a brief summary of the main characteristics, in a media context.

Broadcast	**Point-to-point**
– used by traditional media: radio, TV, newspaper, ... – everybody gets all the information – selection is performed locally – the sender does not learn about local selection (what, where, when, for how long, ...) – requires synchronisation between sender and receiver	– used by websites, IP-based radio/TV, apps, ... – selection is centrally visible – only the information that you select is sent to you – enables two-way communication – enables personalised services – enables monitoring / profiling / surveillance

Point-to-point communication is much more efficient, in the sense that only the requested information is posted. For instance, I never read the sports pages in my newspaper; they go directly into the bin. In another sense point-to-point is more wasteful, since if many people want to access the same item, it has to be sent many times, to each one individually — instead of just once, like for broadcast. Indeed, news-servers are sometimes overwhelmed by the many requests, and actually stop working.

There is a clear trend away from broadcast towards point-to-point communication. Partly, this change happens automatically, as many new services appear that are only offered via the web or via apps. But existing services that are traditionally offered in broadcast mode are becoming point-to-point, like television. The main advantage for the service provider is that it yields insight in the behaviour of the user and thus enables additional, personalised services. The main advantage for the user is the asynchronous character of point-to-point: the information can be obtained any time, upon request, and not only at the moment when it is broadcast. The main disadvantage for the user is loss of privacy, and possibly also loss of 'objectivity'. This is discussed below.

Personalised services

All companies want to reach their most likely customers, via advertisements and direct offers. Advertisements in the broadcast model are also broadcast to everyone and may thus reach — and annoy — people who are not interested. With point-to-point communication it is possible to target advertisements, so that only specific users receive them. To appropriately target messages in point-to-point communication you need to know who is on the other side of the line. Therefore the advertisement sector builds profiles of customers with commercially relevant information (salary, hobbies, age, sex, purchase history, friends, *etc.*). Some companies urge you to always log-in so that it is easier to track

your activities, but others link your activities via other means like cookies, IP-addresses, browser-fingerprints, *etc.* This "behavioural targeting" raises serious privacy concerns. But also there are worries about unfair discrimination.

The advertisement sector cunningly portrays this targeting as a valuable, almost altruistic service that is in your own interest: "You only get advertisements of goods that you are really interested in!". But, of course, this is a form of framing. They only send you the advertisements that *they* want you to see. Profiling may well be used against you, to offer you a — truly personal! — higher price. Also, certain products, like mortgages or insurances, may not be shown to you at all, because of the perceived high risk based on your profile.

Loss of objectivity

An important aspect of point-to-point communication is that service providers can put different versions of the same message on different point-to-point channels, depending on who is on the other end. For instance, some time ago Google started offering personalised search, where the answers to search queries may be different for different people, depending on what Google knows about you — which is quite a lot, typically. Recently, Google started offering personalised maps, where the annotation on a map depends on what Google wants to show you. It is not clear how far this will go or where this leads to. Will Google only show you gay bars on a map if it thinks you are a homosexual?

News sites may learn the preferences of their customers over time and adapt the selection of news articles accordingly. Thus, the topics that are presented to you most prominently are the ones that you often read about. This may be convenient, but also makes life more boring because you will no longer be confronted with the unexpected.

Maybe, at some stage, news articles themselves will be adapted to their readers: very brief for some, longer with more details for other; factual for some, more colourful for others. Such personalisation of content raises lots of concerns. Which criteria are used for showing me this instead of that? Do (or should) I have a possible influence on these criteria, or even be able to choose or refuse them? How transparent are the evident commercial interests involved? Should this approach be regulated? If each of us gets a different version of reality — and thus lives in his/her own "filter bubble" [6] — what is the consequence for social cohesion or equal opportunities?

A right to receive freely

When other, public or private, parties select what you get to see of the world, they are clearly determining what you receive. This may happen for instance via personalised search, or via personalised news selection. This steering of perspective may limit your options and thus affect your autonomy. As already discussed, the right to *send* is historically protected via free press/print clauses in constitutions. But what about the right to *receive*?

In 2010 a constitution reform committee [7] in the Netherlands recommended to update such free print clauses in the constitution, to the two clauses: (1) no advance permission is needed to publish thoughts or opinions, barring everyone's legal responsibility; (2) the receiving of information is free, barring restrictions set by law. These proposals are interesting because they place sending and receiving on equal footage — but they have not been adopted yet.

The question remains: how should such a freedom to receive be interpreted? Does it mean that I have a right to unpersonalised information? The main task of a news-provider is to collect and select information about what is going on. Thus, selection is part of the job. The question is if making these selections personal should be optional, for the receiver. Many democratic governments support or protect pluriformity of the media, so that citizens can have access to a broad spectrum of information. It seems that personalisation of media reports is undermining this pluriformity, at least on a personal level.

Another question is whether 'freedom to receive' means that we have a right to consume the news, read books, *etc.* without being monitored, that is, without the sender recording what we precisely read/watch/hear, when, where, and how long. This applies for instance to news websites, but also to e-bookreaders and mobile devices. Continuous monitoring on point-to-point channels, and updating of profiles, may have a chilling effect, reducing the pluriformity of choices.

3 Conclusions

This essay discusses several new developments that result from advances in computer and network technology. Many of these developments have been described elsewhere, in one form or another (see *e.g.* [4]). What is new here is that they are presented from a simple coherent perspective, namely as consequences of two grand changes: the separation of carrier and content, and the shift from broadcast to point-to-point communication.

Postscriptum

The basis of the text presented here is an article [2] written in Dutch. It was reorganised into an invited presentation at the 8th International IFIP Summer School on Privacy and Identity Management for Emerging Services and Technologies in June 2013. The current version concentrates on the two most prominent changes identified there. I am thankful to all those who provided feedback, including the referees.

References

1. M. Aid. The NSA's new code breakers. *Foreign Policy National Security*, 21(11), 2013.
2. B. Jacobs. Bedwelmende zelfontplooiing. In T. Kwakkelstein, A. van Dam, and A. van Ravenzwaaij, editors, *Van verzorgingsstaat naar waarborgstaat. Nieuwe kansen voor overheid en samenleving*, pages 85–97. Boom, 2012.

3. E. Morozov. *The Net Delusion. The Dark Side of Internet Freedom.* PublicAffairs, New York, 2011.
4. E. Morozov. *To Save Everything, Click Here.* Allen Lane, New York, 2013.
5. N. Negroponte. Bits and atoms. *Wired*, 3:01, 1995.
6. E. Pariser. *The Filter Bubble.* Viking, 2011.
7. Rapport Staatscommissie Grondwet, 2010.