

*Freedom of the Media and the Internet*  
*OSCE, 13-14 June 2003, Amsterdam*

**COMMUNICATION, CODE AND CONTROL –  
The Privatization of Media Regulation and Censorship**

Dr. Christian Ahlert, Programme of Comparative Media Law & Policy at Oxford University

The prime consensus when it comes to the question whether communication can be regulated on the internet was, and still is: the internet interprets censorship as failure and routes around it. A not only unfortunate, but rather dangerous mixture of technological determinism and judicial pessimism - resulting in the myth the internet would be immune against restrictions on speech set by a single actor. To make matters worse this chain of logic has led to some rather shrouded presumptions: governments cannot regulate the internet, no matter how hard they would try; and if they would try it would destroy the new freedom the internet has brought to democratic communication. So instead of discussing who should protect our liberties online, we have resorted to the belief that self-regulation is not only the only possible form to regulate the internet, but that it is inherently better than any regulation by the state.

I think this is an argument worthy of deconstruction in sight of what surely should be our shared goal: protecting freedom of speech and expression online. So let me start by telling you a short story. A story coming from a different medium, but useful to illustrate what is wrong with those shrouded presumptions: Let's imagine everybody living in Amsterdam would all of a sudden not be allowed to make telephone calls to the UK. If you would dial a number in the UK, you simply would get a busy dial tone. And nobody would give you an explanation, why you are banned from calling across the channel. And as the story goes, it is British Telecom who would have simply decided, without giving a public statement: calls coming from Amsterdam, will be unanimously blocked; because they must not reach customers of BT. I think the citizens of Amsterdam would have been outraged, and rightly so.

But this story is fortunately just the product of my imagination. Unfortunately the next story is not, and it represents "a clear and present danger" to the freedom of speech on the internet: Some weeks ago every user of Oxford Universities email system was blocked from sending emails to anybody with an AOL email address: When you sent an email to an AOL user, it simply came back, leaving the impression the email-address was wrong. But it was not the address that was wrong, it was AOL who had decided to block any email coming from Oxford.

And in contrast to my imagined example almost nobody was outraged, because it appeared as a technical mistake, but communication was effectively blocked in between Oxford and the AOL community of 20 something million internet users.

So what can we learn from this example? It illustrates how effective, those who control the infrastructure of the net, can control the way we communicate. A private party had decided, because it had received spam from an Oxford address, to block and punish all Oxford users. It represents a form of private censorship not tolerable in other media. It was not transparent to the user, indeed it was invisible to the user, and therefore he could not hold AOL accountable.

It shows that Internet Service Providers control an important part of the internet's infrastructure: they can block email, filter websites, monitor traffic, they can see who is surfing where, when and how long, they can also take-down websites so that they diminish from the web.

But the argument I am making today is not about AOL blocking emails, or the power of ISPs; it is an argument about the relationship of technology and control in networked digital media.

And it is an argument about a double misconception: First, that the internet by design is good for the freedom of the media, and second that no control by governments means that nobody controls the internet.

When it comes to the internet and freedom of the media, the state has withdrawn itself in many cases from protecting the freedom of expression, speech and the media, in favour of self-regulation by industry. And that is dangerous for at least two reasons: First, it has lead us to promote self-regulation of the internet, often for the wrong reasons and without understanding fully its consequences. Secondly, it has lead us to a misguided understanding of how the internet itself regulates communication.

My main argument is then: only if we understand the underlying technology of the internet, we will understand how freedom of speech and expression needs to be protected online.

It is undeniably true that the internet is a great medium for free expression, because of the way it has been built and designed. But this must not be the case in the future. The internet has matured, and so have strategies and concepts to control, censor and regulate it. Hence we have to look carefully where the architecture of the internet is vulnerable against censorship and where the parts of the internet that make the "control of communication flows" difficult are being rebuilt to regain control.

My first example illustrated how powerful Internet-Service-Providers are. They are so powerful because of their central place in the architecture of the Internet. And it is this architecture we need to focus on. It is determined by standards and protocols and written into the software code of our computer programs. It is build into the backbones, servers, routers and the computers we use that make up the internet.

On the Internet – the rules that enable, or restrict our capability to communicate, receive, distribute and share information are written into "Software Code". And this software code not only makes our computers work, it also tells our computers how they work. And at different but interconnected levels in the computer environment rules can be written into this "code" – as Larry Lessig famously has illustrated with his phrase that "Code is Law".

While the current design of the internet infrastructure makes file sharing possible, copying easy, and censorship difficult, all this can not only be different, but will be written into the rules of that medium. It is crucial to understand whether a new protocol for the internet makes censorship easier, or whether it might add to the erosion of privacy when communicating online.

To understand this is even more crucial, knowing that this year marks the first time in the history of communication that more digital communication devices will be sold than analogue. More pictures, books, music, personal communication will be digital and distributed online than ever before. And as more and more communication and other forms of

social transactions are performed online and digital an enquiry into the characteristics and extent too which “Computer Code” controls communication, and how we then should vice versa control the producers of this Code, becomes important when discussing the freedom of speech and the media.

So whereas my first example focussed only on the “hardware infrastructure” level of the internet; my second example will highlight why “freedom of the media” also needs to be protected in the other layers of digital technology.

We like to think that we are in control of the way we communicate via our computers – at least most of the time. But imagine somebody would change the software and hardware of your computer in a way that you cannot “copy” and “paste” anymore.

And this is not my imagination: Intel the biggest chipmaker of the world is working on a product called “Trusted Computing Platform Alliance”. Intel claims that this is “a new computing platform for the next century that will provide improved trust in the PC platform”. And Microsoft wants to incorporate into future versions of Windows a software called Palladium.

The underlying rationale is fairly simple: more and more content is being distributed digitally and hence there is a desire by industry to be able to better control the distribution of that content. Hence computers using these technologies will include a digital encryption and signature device. So that the computer can decide, based on the users’ authentication, what data you can access, how and to whom you can pass it on.

There are plans to use the same software structure for email and documents - resulting in emails that may disappear in two weeks, or documents that can only be read on the computers in one company. You will not be able to turn this new functionality off, as it will also be built into your hardware. Some of the proposals even contain plans to monitor your computer; and when you will download an illegal file, it will either be remotely erased, or your computer will be turned off.

So what does this tell us? Technological choices regulate the way we can communicate via the internet, and these choices are currently being made. On a day to day basis by ISPs and for the long run by the computer industry. At different levels in the infrastructure choices will need to be made about who can control and to what extent the way we communicate.

And the problem is not that whether this will happen, or not: The problem is that these “regulations” are being built without public debate and that these seemingly technical regulators are not held accountable. So the future of the freedom of the media online will rely on the insight that when it comes to the Internet and digital media “seemingly narrow technical choices can have a broad and lasting impact on public policy and individual rights – more so even than traditional policy processes”. And these choices are choices about digital technology that can potentially regulate communication far more perfectly than it was possible in analogue media technology.

At the same time these seemingly technical decisions are not being made within governments and international organizations, but in private bodies – such as the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), or the Intel led Alliance for trusted computing – that set technical standards for the Internet. But those and other key standards

bodies operate largely outside of the public eye and with little input from public interest groups or policymakers.

So let me then conclude with a perhaps boring, but important point: Technical systems incorporate 'political properties' and the code and standards design and implementation processes for the internet are 'regulative mechanisms' which have to be examined in detail in order to understand their various and subtle impacts on the way we are able to communicate online. If we then want to make the right choices about the regulation of the digital media, we will need to understand that "technology matters".