Do we need new rights in Cyberspace?
Discussing the case of how to define on-line privacy in an Internet Bill of Rights

David Casacuberta
Universitat Autònoma de Barcelona
Departament de Filosofia
David.Casacuberta@uab.es

Max Senges
Universitat Oberta de Catalunya
IN3, Internet Interdisciplinary Institute
maxsenges@gmail.com

Abstract

During the early days of Internet it was widely defended that being in an on-line environment clearly transformed some human rights; and might even create new ones. We argue for the consideration of an Internet Bill of Rights (IBR) however rather than inventing new rights, we propose that some rights have to be reconsidered within the emerging virtual context. Privacy, anonymity, freedom of expression, and so are not exactly the same rights we have in the realm of our physical being. What changes are some inarticulate contextual conditions, which make some people think that rights are actually changing. This has theoretical implications. We attempt to show that there is no need to re-think rights like privacy from the beginning, or even eliminate it, as some scholars propose. It also has implications for policy making, as it provides a general methodology to consider and adapt to virtual contexts in order to assure that basic human rights can be correctly applied and defended in cyberspace.

Key words: digital technologies, information society, privacy, virtual versus real, new rights.

Resumen. *¿Necesitamos nuevos derechos en el ciberespacio? El caso de cómo definir la privacidad en línea en una declaración de derechos de Internet*

Durante los primeros días de Internet, era común defender que formar parte de un entorno en línea claramente transformaría los derechos humanos, incluso podría crear nuevos. En este texto, queremos argumentar que, a la hora de establecer un *Bill of Rights*, o declaración de derechos en Internet, en lugar de definir nuevos derechos, necesitamos reconsiderar los que ya existen dentro del emergente contexto virtual. La privacidad, el anonimato o la libertad de expresión, entre otros, no son exactamente los mismos derechos que tenemos en el reino de lo real. Lo que cambia son ciertas condiciones contextuales no articuladas, que hacen pensar a algunos que son los derechos los que han cambiado. Ello tiene ciertas implicaciones teóricas. Intentamos mostrar que no hay ninguna necesidad de repensar derechos como la privacidad desde el principio, ni mucho menos eliminarlos, como algunos analistas proponen. Igualmente, tiene implicaciones para el desarrollo de políticas, ya que ofrece una metodología general para ser considerada y adaptada a los contextos virtuales, para así poder asegurar que los derechos humanos básicos pueden ser correctamente aplicados y defendidos en el ciberespacio.

Palabras clave: tecnologías digitales, sociedad de la información, privacidad, intimidad, virtual versus real, nuevos derechos.

Sumary

Why we need an Internet Bill of Rights

When the first philosophical essays started to consider Cyberspace, most were fascinated by that famous oximoron of «virtual reality» and start to dream about how life and being would change. Sherry Turkle (1997) analysed how the possibility to create several on-line identities might change our whole approach to live. Other authors like Rheingold (2000), Haraway (1985), Hayles (1999) or Grey (2002) made similar claims about society, gender, arts or politics. However, cyberright activists as well as scholars who were more interested in applied issues like Lessig (2000), Castells (1996), Livraghi (2000) or Jenkins and Thorburn (2003) prefered to stick to a more conservative analysis and outlook. They find many similarities and little differences between being in real life and in the on-line world. A common quasi-proverb of those law and ethics pioneer days was: «What is legal in real life should be legal on the internet. What is illegal in real life should be ilegal in Cyberspace».

Only a few people still believe in the revolutionary transformations expressed by e.g. Barlow's (1996) utopian Declaration of the Independence of Cyberspace. Largescale profan everyday use has watered down a lot the utopian claims from the optimistic pioneers. The debate continues deploying the methodology and argumentation of applied philosophy. Even when we accept that pragmatic line of simply interpreting cyber activity in the same legal system, there are various contextual factors unique to Cyberspace that have to be understood and dealt with.

Clearly, as more and more people live (partially) in Cyberspace, the urgency to properly understand how Human Rights can be protected in this virtual realm grows. In order to create a Human Rights based regime (Jørgensen, 2006) in cyberspace, in which netizens are protected against arbitrary action of system operators of public sites, as well as public institutions as such[1] an Internet Bill of Rights is needed in order to clarify and in some cases extend the established Human Rights, taking the particularities of cyberspace into consideration. How this Internet Bill of Rights should look like, what type of questions should it address and in which way are the main subjects of this paper.

1. It is our understanding that the ratification and implementation of the proposed Bill of Rights would be initially voluntary and let by public institutions.

The clash of rights in cyberspace

It is understood that in Cyberspace in some aspects unprecedented axiological dilemmas emerged, and hence there is a need for defining a new normative framework which complements the existing Human Rights. A dilemma arises whenever there competing values create a paradoxical situation in which all possible solutions neglect at least one legitimate claim, demanding for a establishment of priorities.

Being the result of the work of educated and civilized scientists, cyberspace emerged embodying liberal norms and values that evolved in auto-regulatory practices. Additionally we can observe the non-neglectible influence of the cultural movement happening especially in the very active Bay area during the sixties, which accompanied the de-regulatory and participatory processes. While the advantages of auto-regulation, and especially its adequacy in consideration of the changing conditions due to the fast technological development of cyberspace, are recognized, it is our intention to argue for the benefit of developing the architecture of international agreements dealing with the multitude of aspects that need to be organized (e.g. security, e-business, SPAM, etc.), based on constitutionally stipulated (traditional) Human Rights, illustrated and complimented by guidelines dealing with special conditions of cyberspace. Or put differently, we recognize auto-regulation as the most agile regulation method, but some issues (as defined by the Working Group on Internet Governance[2]) are not likely to be taken up by private actors or are likely to be resolved unjustly as the lobby interest of the private sector clash with those of the public (civil society). It is for those cases that global solutions, political institutions such as a Bill of Rights is needed to enable deliberation and consensual agreement for how to find fair arbitration.

The following lists some examples for specific cases of clashes between rights in cyberspace[3]:

— Freedom of expression versus minority rights (hate and racist speech).
— Economy of attention model (Google, Yahoo, and their economic model of selling ads based on the profile of user) versus privacy of users.
— Right to know (Hackers and computer scientists) versus right to privacy (server administrators and owners).
— Right to know (Hackers and computer scientists) versus copyright and patent rights of companies and creators.
— Right to have our equipment protected (computer security) versus the right of companies to keep their code secret in order to hold their copyright and patent rights.
— Anonimity in cyberspace for users versus the need to identify oneself in e-commerce transactions.

2. <http://www.wgig.org/docs/book/Appendix_II.html.>
3. Some of the dilemmas are due to the specific conditions of cyberspace — like the non-availability of identity cards as verification of maturity, others like the securing of and limits to privacy in the eye of public interest have a long history and are traditionally much disputed issues.

— National security (tracking cybercriminals, terrorists, and so on) versus privacy of users.
— Right to cryptography (privacy of users, trustability of e-commerce operations) versus the need to know for government agencies.
— Freedom of expression versus trustability of media (both mass media as well as independent media, including blogers).
— Right to access (including p2p networks) versus fight against piracy.

As it is commonly done in most human rights literature, all these problems can best be solved by developing some sort of «rights ranking» which may let us know, case by case, which right is more important, always based on a context. There are no magic solutions like: «Freedom of expression is more important than privacy». Instead a careful analysis of context is always needed. However, it is important to assume that some sort of ranking is necessary and that, therefore, sometimes, some user right might have to be temporary cancelled in order to protect a higher right from another user. From that point of view there are no methodological differences between internet and real life, so we won't continue analysing this here. In this contribution to the discourse about an Internet Bill of Rights we attempt to establish the necessity for such a proposition which allows for a mutual settlement regarding dilemmas inherent in social systems created in cyberspace.

Is it really needed then? What point are we trying to make when arguing for an Internet Bill of Rights? The meaningfulness and possibilities of an internet governance system is not far-fetched. It seems adequate at this point to stress the relevance of the pioneering multi-stakeholder approach to internet governance as a precedent for the collective management of global Common Public Pool Resources (CPPR, Ostrom, 1990) like physical logistical infrastructure or potable water. The case of internet governance is un-precedented in its mode of participation, but at the same time participants (especially the new players of civil society) should prudently respect and embrace the experience the traditional negotiators of international agreements contribute to the process. Valuable insights can be drawn from historical solutions of CPPR and public-good management solutions.

Then of course, besides the practical questions of how useful it would be for a future governance system/commission, there is the methodological issue of how an Internet Bill of Rights should look like and, specially whether some rights might dissapear or at least change in a digital context. To properly understand the possible differences the provision of inalienable Human Rights in Cyberspace two practical prerequisites shall be mentioned.

We agree with the notion that in Cyberspace software code and hardware properties (the technological *gestell*[4]) are law (Lessig, 2000). Technological

4. Under technological gestell we understand —following Heiddegger— the soft and hard infrastructure building cyberspaces environmental conditions and implementing/manifesting the procedural rational of its stakeholders.

gestell describes conditioning factors establishing the rules for being in Cyberspace. These rules depend on the one hand on the finalities and ideals pursued by its citizens and on the binary feasibility (whether the solution is digitally expressible) on the other hand. The former aspects are traditionally dealt with in social systems by human institutions negotiating the normative priorities and consensus among conflicting interests, while the search for technological solutions is informed by and needs to comply with the normative framework, there is a mutual interdependence between the two. Let us look at the case of the clash between privacy and e.g. the protection of children regarding explicit adult content. Some sort of identity management system is needed in order to verify user age as access condition for this kind of content. While this normative objection is clear, the need for privacy restrains the possibilities for such an identity management system. Hence either one right has to be defined as more important than the other or a technological solution needs to be found. For these purposes (and once the pure free market model is ruled out) three closely collaborating institutions can be thought of: one for the transparent and inclusive discourse about the normative guidelines, one for the agreement of open standards of the technological, and one for the arbitration in case of colliding interests and enacted conflicts. In other words one leading social-normative institution — as presently emerging in the IGF; one leading standardization institution — as presently embodied by the IETF and the W3C; and one institution that can be appealed to in order to judge disputes — as the presently emerging International Criminal Court to gauge general rights controversies and infringements.

Given the importance of the informational and discoursive function of cyberspace[5] all humans need to be able to access and participate. Subsequently it makes sense to conceptualize cyberspace as a global public good or common public resource. The former resulting in a right to access the later in the need for fair spectrum distribution mechanism allowing for allocation of spectrum considering all stakeholders legitimate rights and not based on monetary competition[6]. While political agreements (negotiated in a multi-stakeholder discourse) are necessary for the spectrum distribution, governmental investment is needed in order to provide adequate public access points for citizens. Put differently all humans should have a right to non-competitive minimal access to cyberspace.

While markets based provision of internet bandwidth access has evolved as effective modus operandi and the price differentiation of bandwidth provided serves as incentive to push performance improvements, network neutrality represents an essential condition for creating a just discourse environment, enabling debate without biasing the deliberation process through content discrimination based on wealth based power. Hence network neutrality shall be

5. Understood as the converged sphere comprised of todays internet, television and telephone networks.
6. See CRIS campaign for more information on fair spectrum distribution.

a condition defined and stipulated in the Bill of Rights. By Network neutrality (equivalently «net neutrality», «internet neutrality» or «NN») we should understand a principle applied to residential broadband networks, and potentially to all broadband networks. Precise definitions vary, but a broadband network free of restrictions on the kinds of equipment attached and the modes of communication allowed would be considered neutral by most advocates, provided it met additional tests relating to the degradation of various communication streams by others. Arguably, no network is completely neutral, hence neutrality represents for some an ideal condition toward which networks and their operators may strive. [http://en.wikipedia.org/wiki/Network_neutrality]

Another issue already touched upon is the right to privacy that is various times in conflict with commercial and security interests. Here personal liberty and privacy are assessed to be axiologically dominant. As defined in the Human Rights, all individuals have a right to privacy. This right shall include ownership of produced data as well as the right to cryptography, as is the more feasible solution to protect personal data in the open architecture that Internet has today. In practical terms this translates into the obligation to inform about the act and kind of data recorded as well as to anonymization or optional removal of personal data trails (data shadow).

Last but not least let us consider the complex of issues involved in the right to freedom of expression. As raised above there are dilemmas with the rights and responsibilities of a platform provider being in conflict with the rights to access and free expression. As implicitly stated in the right to privacy everybody has the right to private conversation and thus everybody has the right to create and participate in exclusive private environments. In contrast sites open to the public shall provide public cyber rights and comply with public norms. While the actual content falls under freedom of expression maturity has to be established and discussion possibly including (democratic) collective assessment regarding the nature of the content would certainly improve the informational hygiene while not infringing heterogeneity and liveliness. The first problem of anonymous verification of certain identity aspects like age seems to be feasible through solutions like shibboleth identity management. For the second dilemma we would like to contribute a scenario framing a solution.

Lets imagine the institution managing the cyber address assignment includes meta-information regarding the content of the information and service provided. This would enable, for example, the classification of content to be only appropriate for mature users as well as the insertion of a informative page advising the user of the quality of the content. This upstream page would also allow for public discourse and collective assessment of content provided at the site. This way there is no enforcement of particular axiological dispositions in the form of restraining the freedom of expression but vulgar and extremist content would be classified and debated.

From ideal to real: the case of cryptography

In an ideal world, the right to privacy would be protected by an entity with full understanding of the priorities of rights and capable in each situation to decide which right is more important. This entity also needed total knowledge of the context to be considered in order to produce the ethically correct or at least most suitable solution. Because this is impossible from a practical point of view, the basic need is to find a middle way between autoregulation and institutionalized control. The Internet Bill of Rights should therefore primarlily declare cyber-contextualized Human Rights, and then leave the concrete institution building and practices for policing the rights to a separate discourse.

In this section, we will make an extensive use of real life (that is, non digital) examples of privacy to build our notions of how to deal with privacy and establish why cryptography is important for that right. The main reason is precisely that our intuitions on how privacy should hold in a virtual world are still too young to be trustable.

A first step in this direction is to distinguish privacy from the concept of secretism. Privacy is not about keeping something dangerous or even criminal hidden in order to avoid prosecution. That is the reason that a terrorist, a drug dealer or peadophile might exploit cryptography: to keep their criminal actions hidden from public view. But this is not privacy; this is secrecy. Therefore, the common argument from some governments stating something in the line of: «Hmmm… So you need cryptography you say? What is it what you are trying to hide?» is completely unacceptable.

Then we must distinguish —from a psychological point of view— privacy from intimacy. Privacy is a more general subject, that simply states the right of the citizen to decide when a third person has access to his/her own communication, documents purchases in the Internet no matter whether they are of an «intimate» nature in a psychological term.

One of the main arguments to prohibit cryptography is precisely that it can be use for secretism. This is certainly true: terrorist, drug dealers, paedophiles and other classic evils that the press likes to imagine roaming free in the wilderness of Internet do use cryptography to hide their criminal actions. The question is not if cryptography can be misused. Of course it can be misused. Email can also be misused to send death threats, hate speech, or viruses, but no one is asking to forbid email. So the question is: is cryptography main use secrecy or is it just one possibility among many more rational uses? Moving to real world; cryptography is like shades we use at home for privacy but can also be used for secrecy? Or is it more like entering a bank wearing a ski-mask which will inmediately trigger all alarms? We argue that the first case is true: it is very difficult to imagine an online world without some sort of cryptography.

The next step is to realize that most internet-related rights (and that includes of course privacy) are very context dependent. The right to live shouldn't be dependent of any context (despite the fact that some countries which have

death penalty think otherwise). However, the right to privacy is clearly dependent on contexts. Here are some:

It depends on:

— The way the law views a particular individual: my right to talk on the phone or to send an e-mail to someone else without a third party eavesdropping my conversation is not absolute; a judge might consider that I'm a criminal and therefore produce a warrant to get my phone or email conversations monitored.
— It depends on the will of the owner of the right. I might decide to keep my e-mail hidden from third persons but I also might decide to freely publish it in the Internet.
— It depends on where I am: If I'm at home, with windows closed, no one knows what I am doing, but if I'm in the middle of a crowded square this privacy is lost.
— It depends on an identification process. Let's return to the crowded square. Even if people see what I'm doing in that crowded square, if that crowded square is in a foreign country in which nobody knows me, I still retain much of my privacy, as they might see what I'm doing, but nobody knows who I really am.

Clearly, privacy is created after a psychological process, and depends on culture. Despite some exceptions, like kamikazes, it is very difficult to find a person or a culture in which living is not considered a supreme value. However, several philosophers and historians do believe that the concept of privacy was inexistent before the middle ages, and there are even cultures today that do not seem to consider privacy at all.

In 2000, in an invited talk to the Computers, Freedom and Privacy Meeting, eminent science-fiction writer Neal Stephenson argued for the existence of several models to react to privacy attacks. Basicly, he stated that citizens worry about their privacy when there are no more basic rights at stake. They need to feel safe. When the environment suddenly turns dangerous, citizens might still not accept a «big brother» model, but might feel comfortable in the idea of a multiple vigilance system in which the process of control is distributed among several organisations. For example, instead of an onmimode police state, you can have your neighbourhood controled by a private security company, the city police to guard the streets, another private company in charge of security in airports, and so on. Stephenson calls this model a «domination system» following the ideas of the christian pacifist Walter Wink (2000). What interests us more here is the idea that:

a) the value we give to privacy might change depending on the context: if suddenly our neighborhood becomes a dangerous place due to a rise in crime, probably our concerns about privacy will start to evaporate and we won't mind anymore the idea of having a third party asking for an ID to anyone trying to reach our neighborhood.

b) Despite the fact that both are attacks to our privacy, we consider more agravating a «big brother» model than a «domination system». Both facts really imply the dependence of psychological process and contexts to understand privacy properly.

In a similar venue we can consider Brin (1998) and his idea of the «transparent society». According to Brin, privacy nowadays is impossible: e.g. streets are full of cameras recording our movements in the public space. All our movements in the Internet can and in fact are recorded in several servers. Our emails can be easily read by the system administrator. But, this might be after all a good thing, because technology gives the possiblity to counterattack using the same coin. We can use video-cameras to record police commiting abuse of authority —like the (in)famous Rodney King case; hackers can use their knowledge to enter in databases of the governments to show the world unaceptable operations. So he argues for what others have called «radical transparency» (Wired, 2007), the positive effects that complete public disclosure leads to more ethical conduct. Brin position might be somewhat naive, but both Stephenson and Brin shows us how dependent of public perceptions of possible threads and replies to that thread might change completely our view of what is privacy and whether we have a right to it, after all.

Another interesting aspect is how the threat to our privacy depends greatly on the way it is produced. It is interesting to observe how much more people worry about surveillance cameras and a lot less about getting their communication being monitored on the Internet. A free email account is enough for lots of people to give away their privacy; and some preview of porn might be enough to open your computer to malware which might be used in the future to register your movements in the WWW. However, people feel usually uncomfortable in the presence of a camera. There are several opposing movements to the use of cameras for surveillance purposes, even artists groups, like the performers Surveillance Camera Players (SVC, 2007) or the Steve Mann's projects about «Subjectrights» in which everybody is invited to record security cameras with their own cameras, following Brin's philosophy (Mann, 2007).

Once all this information is reviewed we can consider, what type of right is privacy? Our proposal is that if we just move privacy from the real world to the Internet we might be forgetting something. Because most rights depends on context, we can evaluate a right as long as we consider the context. But what if we have a context that is so ubicuous that consider it for granted? If we move to a very unfamiliar territory (as it is moving from real life to Internet) we might suddenly discover that the facts that we consider for granted do not longer hold. Does that mean that «new rights» emerge? Not al all; it only means that we are not giving proper attention to the context elements as it should be.

The philosopher of language John Perry (1993) has an excelent term to consider this problem. He calls it, the «inarticulate element». An inarticulate element is some piece of world information that doesn't show up in a conver-

sation, because the context grants it, but without it the sentence the uttering is not meaningful. One example is the concept of «time zone». When I ask a person in the bar: «What time is it?» and she replies «It's seven thirty» all the conversation has an inarticulate element embebbed: «What time is it [in this time-zone]?». Of course, it would be quite silly if she double checked: «Hmmm.. sure! In what time zone are you interested?» But the fact that this element is after all meaningful can be easily seen when we consider another normal conversation like:

1) Hmmm… I should call him, but wait. Do you know what time is it in New York right now?

   Here the inarticulate element becomes articulate: we are asking for time in an specific time zone. Now let's move to the Internet. Two people are chatting and decide to continue the talk later. They propose a time:

2) Ok. We should meet again. What about tomorrow at 13.00?

   However, they connect at different times and don't meet after all because they didn't realise that they were in two different time zones. Does it mean that Internet creates a «new time» or that we need to revise our concept of time? Not all all, it is just Internet doesn't guarantee anymore the fact that two people having a conversation are actually in the same time zone. You need to articulate that element in order to assure proper results. And this is what an Internet Bill of Rights could facilitate.

In the case of privacy we have several inarticulate elements in the real world which we need to consider: We know that in a foreign city it is quite unlikely that people will recognize us. We assume that a letter enclosed in an envelop will only be read by the author, the adresee and the people that he or author decides to share the letter with. We almost never consider such elements unless the situation is strange enough to obligue us to do so. We are in a foreign city but we know that some neighbours are also there on holiday, so we take extra precautions in order not to encounter them; we know that the mail system in a country is not trustable, so we never use it to send sensitive information about us.

Internet challenges all these assumptions. Internet desarticulates the inarticulated elements we consider for granted. That doesn't mean that digital technologies make privacy impossible, as Brin claims. Neither does it imply that we need to consider to invent a new right. Far from it. It only means that conditions are different and that we need to reconsider them before talking about securing the right to privacy on the Internet Therefore, an Internet Bill of Rights should include:

1. A list of rights depending on their importancy, stating which one should be prevail and why in a clash situation.
2. What are the key inarticulated elements that define a right in any given real life situation and which of those inarticulated elements do no longer hold in a digital technology context.

3. An instrument or series of instruments, legal, political, technological, or otherwise that reintroduces those inarticulated elements into play, and guarantee that the rights hold in a similar way.

In the case of privacy, the instrument that is most likely to work to assure we have our inarticulated conditions back is cryptography. Why is that? Let's review what we have discussed so far.

As we said before, privacy depends on several contextual elements. One is the relation to identification. In the real world I have several elements that allow me to consider that I can be identified or not. As we said before, I'm in a foreign city and nobody knows me, or I'm at home with all the windows closed, so I can't be seen at all. But then, there are some situations in which I know I can be clearly identified. I'm in the balcony of my appartment, or I enter my favorite pub, the one I've been visiting for years. By changing the context I (partially unconsciously) decide whether to identify me or not, and then act accordingly. Cryptography using the public and private key system gives me the ability to sign a message so the recipient can check whether it is actually from me or not (For more information about the subject see Schneier, 1993).

When cryptography is used commonly when navigating through the WWW or when sending emails, it gives us the same security that real life gives us de facto. We don't use cryptography at home to talk to our spouses because we know that nobody is listening. That condition -that inarticulate element- doesn't hold in the Internet, so we need to use an instrument to return that inarticulate element back.

Cryptography also gives the «object» to think about when we ponder about our privacy online. Some years ago, almost every privacy activist and lots of people concerned with their privacy in a digital context used to sign their emails. This probably didn't make much sense in principle, as very few people actually did have cryptography like PGP installed in their computers, and only a few of them actually checked the identity of the sender. But as psychological way of making the subject of privacy known among other users it worked quite well, in the same way as a camera staring at us while we are walking freely in the street gives an eerie feeling.

Now we can also understand why the visions from Brin or Stephenson are wrong or at least only partially right: The main reason that privacy is at danger is not the technology per se. Technology is neither good, nor bad, nor neutral. The main reason we have the feeling that privacy is dissapearing or that it is obsolete (as Brin claims), is that the traditional conditions do not longer hold. Simply because they are inarticulate makes it difficult to realise.

Conclusion

We have presented privacy as our main example, but it is easy to see now how the concept of inarticulate elements can help to analyse some of the

other dilemmas specific to cyberspace we list in the beginning. Surprisingly enough —or maybe not— most of them depend on identification processes, so therefore they depend on some sort of crptographic system. Entering a shop and showing my ID should be enough in most cases to assure that I am who I state to be and the clerk can use my credit card to charge me. On the Internet I need to re-introduce this inarticulate element called «visual recognition» by some sort of cryptographic element, plus maybe biometrics. Again, in a world in which publishing was expensive a net of reviewers assured or at least provided some intersubjectivity that could at least guarantee us that a publisher —or the director of the newspaper, or a peer review, etc. did check the credibility of the declarations. In case some falsity was introduced in the information we were receiving there was some company or organization to complain. We need to create similar systems in order to assure credibility of the information distributed plus some sort of identification scheme to recognize that the certificate stating that this information is trustable, generated by so and so, has been really generated by so and so. Again, using cryptography.

The right to know dilemmas usually depend on some sort of identification type also (Are you really a scholar doing a serious research) and again, we can revert to the old conditions (the inarticulate element) using cryptography. However, cryptography is not the only instrument, and not all rights can be guarded using just this measure. A clear example is freedom of speech versus minority rights: here a key technological element might be information retrieval systems, which can be used to detect hate speech and then some sort of legal protocol to obligue the providers of service to remove such type of hostile speech in case that minority rights in this context are more important than freedom of speech of the offenders. And again one of the first steps an Internet Bill of Rights can contribute is to help define what is a private and what a public space online.

References

BARLOW (1996). *A Declaration of the independence of cyberspace*. <http://homes.eff.org/~barlow/Declaration-Final.html.>

BRIN (1998). *The transparent society*. New York: Basic Books.

CASTELLS (1996). *El poder de la identidad*. Vol. 2. *La Sociedad Red*. Madrid: Alianza.

GRAY (2002). *The cyborg citizen: politics in the posthuman age*. London: Routledge.

HARAWAY (1985). *The cyborg manifesto*. <http://www.stanford.edu/dept/HPS/Haraway/CyborgManifesto.html.>

HAYLES (1999). *How we became poshuman*. Chicago: Chicago University Press.

JENKINS; THORBURN (2003). *Democracy and new media*. Cambridge (Mass): MIT Press.

JØRGENSEN (2006). *Human rights in the global information society*.

LESSIG (2000). *Code and other laws of cyberspace*. New York: Basic Books.

LIVRAGHI (2000). *La coltivazione dell'internet. Il Sole 24 hore*.

MANN (2007). <www.wearcam.org.>

OSTROM (1990). *Governing the commons. The evolution of institutions for collective action*. Cambridge University Press.
PERRY (1993). *The problem of essential indexical and other essays*. Oxford: Oxford University Press.
RHEINGOLD (2000). *The virtual Community*. Cambridge (Mass): MIT Press.
SCHNEIER (1993). *Applied cryptography.* New York: John Willey and Sons.
SVC (2007). <www.notbored.org.>
TURKLE (1997). *Life on the Screen*. New York: Simon & Schuster.
WINK (2000). *Peace is the way: Writings on nonviolence from the fellowship of reconciliation*. Cambridge (Mass): Orbis Books.
WIRED (2007). «Get naked and rule the world». *Wired.* March 2007.