"On the Internet, We Are All Pirates, and That's Good"

Interview with Jean-Marc Manach

Francesca Musiani
French National Centre for Scientific Research (CNRS)

Abstract: This interview with Jean-Marc Manach – investigative reporter, specialist of surveillance and privacy protection on the Internet, and a well-known French "hacker-journalist" – explores the issues of cyberconflict and cybersurveillance, focusing on the broad phenomenon of "piracy". In doing so, the interview outlines the different definitions, framings and reconfigurations of those practices, enacted by network users, which have been labeled as "pirate" by different economic and political actors of the Internet value chain. Following Manach's reflections, the interview provides a few benchmarks towards a critical perspective on "piracy" as an ensemble of situated practices which places us, perhaps for the best of our society, in the condition of being "all pirates" of today's digital networks – engaged in the construction and sharing of cyberknowledge.

Keywords: Internet; privacy; hijacking; cybersurveillance; piracy.

Corresponding author: Francesca Musiani, Institut des Sciences de la Communication (CNRS / Paris-Sorbonne / Université Pierre-et-Marie-Curie), 20, rue Berbier-du-Mets, 75013 Paris, France – Email: francesca.musiani@cnrs.fr

Introduction

In the wake of Edward Snowden's revelations about the pervasive surveillance practices enacted by the United States National Security Agency – practices the legality of which is discussed within the American legal system itself – issues of cyberconflict and cybersurveillance have never been so much a matter of "current news". Information and communication technologies, Internet first and foremost, are increasingly leveraged to achieve economic or military objectives – from the theft of critical data to the hijacking of industrial systems. The generalized rise of digi-

tal espionage, tracking and surveillance is unveiled not only by the recent Snowden revelations, or by WikiLeaks' activities, but also by the construction and the organization of an increasingly widespread and lucrative market of surveillance technologies and equipment.

This context also brings about novel ways for the practices gathered under the label of 'piracy'. On the one hand, Internet users and citizens seek to respond to pervasive surveillance via a number of 'bricolage' practices that build, develop, hijack or pirate technical artifacts to secure their Internet connections and prevent third parties to access their data (Musiani, 2011). On the other hand, the development of surveillance and decrypting techniques is a powerful leverage in the development of computing in a "common good" perspective, as history reminds us (Musiani and Schafer, 2011). To understand 'piracy' as a phenomenon – its definitions, framing, reconfigurations – it is important to understand the extent to which practices that have been labeled as 'pirate' by different actors of the Internet value chain, economic and political, are *de facto* largely present and popular amongst users: a phenomenon which places us, perhaps for the best of our society of sharing and knowledge, in the condition of being "all pirates". We have discussed surveillance and its hijackings, digital bricolage and piracy, with "hacker-journalist" Jean-Marc Manach, on November 26, 2013.

Jean-Marc is an investigative reporter, specialist of surveillance and privacy protection on the Internet. For reasons that he details during our conversation, he defines himself as a "journo-hacker". Jean-Marc is mostly known for his blog on Le Monde website, called "Bug Brother", and for his past and present contributions on popular French information websites such as, for example, InternetActu and OWNI. Among his investigations, of particular note is the one that involves Amesys, the French firm which – we learn about it in 2011 – has sold to the Kadhafi regime the surveillance technologies that allowed him to place his opponents under strict surveillance. Jean-Marc is a founding member of the Big Brother Awards France, an award ceremony organized by Privacy International and destined to governments and firms that "do the most to threaten privacy". He has served on the board of *Nos oignons* ["Our onions"], association promoting the development of the digital network Tor in order to "guarantee information, expression and communication liberties". He teaches several courses in journalism schools, on themes of information security and protection of sources. His most recent project (since September 2013) is a WebTV programme on the website *Arrêt sur images*, where interviewees are reached via the Skype programme. His website is jean-marc.manach.net.

***

FM: Let's start with a piece of most recent news. The Pogoplug firm announced yesterday the release of Safeplug, a "49-dollar box" aimed at securing Internet connections of users via a "plug-and-play" Tor. What does your experience within "Nos oignons" tell you about the likely future of this experience? Can the Safeplug box work from a technical standpoint, and be largely adopted by users?

JMM: Technically, it's something that has been done by hackers for a long time now. In this particular case, we arrive at the commercialization of a product, the stage after the prototype. I have a hard time in figuring out precisely the economic potential of this process – if a company can make a profit with this. What is sure, however, is that in the middle of the Snowden affair, this is happening at a very specific moment. One of the problems with the Snowden affair, is that most people will tell one of two things: either "we knew already", or "there is nothing we can do about it". The first point is certainly not true: there is plenty that this affair has indeed revealed or made public; and as for the second, of course not – there is plenty one can do, and could have done even before the Snowden revelations. These, however, have led people to build or experiment with things, both at the micro level and by organizing DIY "laboratories" to secure their Internet connections and prevent third parties (the NSA in the first place) to access their data and wiretap communications massively. At the same time, there are the 'giants', Twitter and Microsoft, turning to HTTPS... This little gadget, Safeplug, is part of a global movement, an effort to secure the Internet again. What is interesting with this box is that it is meant to be placed between the computer and the router – thus, whatever the protocol used, all the traffic is meant to go through Tor – not just Web traffic.

FM: The release of Safeplug is but the latest occasion to reflect upon an issue that has been at the core of my research (Musiani, 2013) – and that of several STS scholars of communication technologies (Aigrain, 2011) – for the past few years: the shaping of decentralized alternatives to the most popular Internet services of today, as a possible way to improve the protection of privacy and the security of one's online identity. What do you think of this "technology-based" approach to security and privacy, and its effectiveness vis-à-vis other strategies, such as written law or user education?

JMM: One of the main geopolitical influences that the United States have exerted on the Internet has been, and still is, the worldwide propagation of the idea that law cannot be trusted. The U. S. is a country that does not trust its institutions: so, for example, it is a lot simpler to obtain information that concerns institutions, most notably thanks to documents such as the Freedom of Information Act. It is a very powerful instrument, which may even allow to declassify NSA documents. A fortiori, with the

Snowden revelations, we have seen how the NSA is indeed violating American law. In France, this defiance vis-à-vis the State may be there, but it is not embedded in the system; however, an increasing number of people, thanks to the Internet, are starting to be careful.

The solution is often thought to be a technical one, given that addressing the issue from a legal standpoint always takes more time. The privacy-by-design (PbD) approach[1] is technical, cultural and financial at once. People have been fighting for a long time towards this objective, but the interest of many firms is still lacking. Here again, thanks to the Snowden revelations, several States and companies will increase their security budgets, and this may, in turn, increase the large-scale adoption of PbD. Snowden has explained that the fundamental reason behind his revelations is that we are experiencing a turn in our conception of human rights. He thinks that, had he further delayed, it would have been too late to know if it is the Matrix that controls mankind or vice-versa, if there is accountability, transparency, responsibility. Maybe it is already too late, by the way. But in any case, we are in the middle of a turn.

This also applies, in my view, to education. A two-year-old child will know how to use an iPhone, while a fifty-year-old adult will need to read the instructions booklet. Well, the reason behind the success of the iPhone, is that there are no instructions to be able to use it. We are in a situation where teachers know less than students, because they were not born with the tools; in addition to this, the former were born in a situation where the act of teaching involves someone who speaks and someone else who listens – not a logic of co-participation and sharing, to which the Internet has accustomed us. Denmark is, to my knowledge, the only country which authorizes students to have Internet access open during their exams: Danes asked themselves why the day of their exam would have to be... the only day of their lives with no Internet access – they understood that the most important thing is not to memorize passively, but to know how to look for, and find, the most useful information at just the right time. I am quite skeptical that we will be able to fully incorporate this vision in our educational system, to set as our main objective the improvement of common knowledge. There are some 'islands'... for example François Taddéi and his Center for Interdisciplinary Research[2]. But overall, I do remain skeptical, especially when I am a witness to the 'strategies' of legislators. A few years ago, to educate children about questions relat-

[1] The PbD idea is developed by the Privacy and Information Commissioner of Ontario (Canada), Ann Cavoukian, in the mid-to-late 90s. It proposes that, as the legal framework is deemed insufficient to ensure the protection of privacy, the latter be introduced directly into the design and the implementation of computing systems and networks (as well as in the elaboration of responsible design and use).

[2] François Taddéi, engineer and biologist, promotes innovation and interdisciplinarity in education and research, especially thanks to the activities of the Centre for Interdisciplinary research (CRI, www.cri-paris.org), which he directs.

ed to copyright violations, they were sending people in schools to tell students not to do this or that – with a similar approach for social networks: don't share too much, it's dangerous! Which is, of course, the best way to make sure they do just that. To discuss dangers and opportunities of sharing at once looks like a more constructive approach to me.

A final point, in terms of education, needs to be made on the difference between the fact of making computing technology available, and making available the infrastructure that actually empowers people to use it. It is of little avail to equip entire schools with laptops if you don't equip them with power outlets and high-speed connections, as well. We need to move beyond our relationship to computers as gadgets if we wish for education to become an actual tool *vis-à-vis* issues of security, surveillance, privacy.

FM: Let us go back in time for a while. You are famous for your investigative reporting work on the themes of online surveillance and privacy, but you said on the occasion of our first contact that you have become a journalist 'by chance'. Indeed, your 'journo-hacker' trajectory (as you define it yourself), is hardly reflecting that of the average journalist. In 2001, you publish a book on French experimental cinema of the Seventies. Your two book-length works, *Big Brother Awards* (Garnier et al., 2008) and *La vie privée, un problème de vieux cons?* (Manach, 2010) [Privacy: an issue for old fools?] on surveillance and privacy respectively, come out in 2008 and 2010. What has led you to become interested in these two themes?

JMM: Indeed. In my early days, I didn't wish to be a journalist: I wished to become part of the film industry. During my days as a university student, I discover experimental cinema and documentaries, and I become passionate about it. I start creating fairly peculiar movies: film festivals didn't want any part of them, because they were too much of a documentary, and documentary festivals didn't want any part of them because they were too much of an experimental movie. So I started to write, just a little bit, because I wished to "defend" my movies. The French *Cinémathèque* was at that moment elaborating a catalog, on the occasion of a big retrospective on experimental cinema, and I suggested to include a chapter on a historical episode that had never been told: the deliberate decision that had been made of not providing any funding to experimental cinema. This article was excluded from the volume, for very opaque reasons of lack of space. I was disheartened by the fact that in a creative milieu such as cinema, thirty years later after the facts I was talking about, it was still possible to censor some things.

At the same time, I was discovering Internet – by chance, I was at the time writing for a journal which had a high-speed Internet connection, which was still very rare; Internet connections were mostly done with 56Kbit/s modems. I was starting to fool around with Web pages, mainly

my personal one. That's where and when it happened: in 1999-2000, I obtain a high-speed access, I start to become interested in the Internet, and that's when the report by Duncan Campbell comes out, talking about the communications surveillance and espionage ECHELON system (Campbell, 1998). My encounter with the Internet happened at the time when I also found out that the entirety of networks was under surveillance. I started to become interested in this from a journalist's viewpoint: to protect my sources. Journalists didn't have any set of instructions to manage this: by turning to the world of hackers, I realized that instead, they did – they knew how to protect their private life, they knew how to use security software. I started to read, then to translate and publish documents of instructions and best practices. That's how I became interested in these topics.

FM: The documentary *Une contre-histoire de l'Internet* [A Counter-History of the Internet], directed by Sylvain Bergère and co-written by you, emphasizes developers and/or activists, and shows the extent to which they have made the Internet what it is today. What was the genesis of this project? What is the advantage of this approach to account for the history – the histories – of the Internet?

JMM: A vast majority of people who retrace the history of the Internet explain that the network was conceived on demand of the U. S. Army to resist a nuclear attack. Well, Internet was conceived just as much by LSD-addicted hippies! This history had never been told before, and documentaries about the Internet were often of the anxiety-inducing type, assimilating Internet users to pirates, hackers to criminals... I wanted to show that it is also thanks to the hackers that we have the Internet. It has, indeed, been funded initially by the American army, but such is the case of Tor, as well – the obfuscation network on which we bestow all kinds of vices today. There is so much stuff we owe hackers – in a broad sense: the promoters of sharing, of the openness of source code, of free software, of an interest in transparency and a keen preoccupation with privacy...

FM: This also entails a re-definition, in the eyes of the public, of what a hacker actually is...

JMM: Very much so. Especially in France, indeed, where the hacker figure has been 'demonized' for so long. In fact, it is the DST [Direction for the surveillance of French territory] that put together the first team of hackers, in the early Nineties, and when this became known, nobody wished to be defined as such any longer. In 2001, I was attending the first French symposium on network security, and half of the attendees were wearing a uniform: the conference was taking place in the very premises of the *Ecole militaire*! We had to wait for 2007 in order to have the first hacker festival of France and the 'coming-outs' of people defining them-

selves as hackers. Last year, France hosted almost a dozen network security-related conferences, gathering internationally-renowned hackers – an unthinkable thing just a few years ago. The 'demonization' of the hacker also helps accounting for several things we have discussed earlier on, the approach of the educational system to digital matters. It also explains why we have been targeted, as TV viewers roughly at the same time, with a portrait of the Internet as a nest of paedophiles and nazis – so ludicrous. But this happens a lot more in France than in other countries, and I think it is linked to the top-down manner in which our State is organized. They have several faults in the United States, but there, if you try to build a company and fail, your chances increase to obtain funding to try and build another: in France, if you have failed, you're busted. That's what the hacker culture is about, as well: to integrate failure into development.

FM: In regards to "dominant histories" and the formatting of discourses that derives from them: we often have the impression, thanks to the way it is treated in the press, that the history of Internet surveillance revolves around the United States. Is it indeed the case, or at least, it it the case to that large an extent? Does this history hide discourses and practices – State-driven, company-driven, or a mix of both – of which we should be more aware?

JMM: We cannot understand the development of computing and networking without understanding that it also derives from the efforts undertaken in order to break secret codes during World War II. The Enigma programme, which had led to the development of Alan Turing's first prototype of computer, is an example of this. The development of the telecommunications industry has paralleled the development of the surveillance of telecommunications. A humongous amount of money has been destined to this development during the Cold War, as well. Internet is the "comet's tail" of all these episodes. Today, the market of telecommunication espionage and surveillance is estimated at 5 billions of dollars per year. These espionage systems were once exclusive purview of intelligence agencies of the biggest countries, like the United States, China, Russia, France. Not anymore. A number of small- and medium-sized companies are proposing services in this field.

FM: Is it the Amesys affair you are talking about? As a reminder, Amesys is the French company that – as we learned in 2011 thanks to your investigative work and that of the Wall Street Journal – sold to the Kadhafi regime the surveillance technologies that allowed him to put his opponents under surveillance, and to monitor the entirety of Internet communications alongside mobile and satellite networks in Libya.

JMM: Absolutely. Today, any dictator, just as any American county sheriff, can buy in a very simple manner any kind of telecommunications

interception devices. People, libraries, institutions, countries: there is a true military and industrial complex that is put into place, including several private contractors – Snowden was one of them. It is a business that was not at all existing at this level before 2001. So, to come back to your question, we speak too much of the U. S. and the NSA, but it is because, paradoxically, it is a country that has a culture of distrust towards institutions, where phenomena such as whistleblowers and the right to declassify secret documents do exist. It is not the case in Russia, or in China.... nor in France or in the United Kingdom, whose governments do, however, violate law in the exact same manner or at least, are heavily suspected to do so. It is, indeed, a paradox: the U. S. are a great democracy, with plenty of people fighting for their individual rights, and that's what allows us to have these documents; elsewhere, we do not have this opportunity, and lacking documents, we do not really know what is the extent of surveillance in our country. One of the lessons showed by Snowden in this instance is perhaps that, in this sense at least, the United States are a better democracy than France is.

FM: The privatization of Internet governance, the important role played by industry, voluntarily or forcibly, in the regulation of content and freedom of expression has been central an issue in my research for quite some time. Beyond Amesys, is this a theme you cross paths with in your work, and how?

JMM: Since the early 2000s, we have spoken about self-regulation, both of civil society and private actors. An interesting example, in France, is the now-defunct Forum des droits de l'Internet [FDI, Forum for Internet Rights], where, precisely, representatives of ministries were gathered with civil society and company executives. This has allowed to avoid some mistakes, and it also prevented several laws from being debated exclusively by politicians that, oftentimes, do not understand neither the functioning nor the capabilities of the technologies they wish to 'regulate'. Since then, the FDI was closed, and the Hadopi[3] law created...

FM: The multistakeholder model is also that of the Internet Governance Forum. The central idea of this arrangement is precisely that we "just" engage in dialogue there, but this dialogue...

JMM: ...allows to avoid a number of missteps! Well, the FDI has helped to a lot more than that, but as one of our invitees for the docu-

[3] The Hadopi acronym stands for *Haute Autorité pour la Diffusion des œuvres et la Protection des droits d'auteur sur Internet* and indicates an agency, created in 2009 thanks to the so-called "Creation and the Internet" law, which is mainly known to have been the first one to administer the "graduated response" or "three strikes" procedure as a means of copyright enforcement.

mentary was saying, "those who talk do not throw bombs at each other". Talking allows to avoid an excessively schematic and grotesque vision of the Other – the contrary of what happened when our former President declared that he wanted to "civilize the Internet", for example. How can one think that this point of view, not dissimilar to that of colonizers, can be applied to the Internet? The extent of this impossibility is highlighted by the (limited and not relevant) practical effects of the Hadopi law: a 150-euros fine, and it was not even the fault of the individual, but of his ex-wife who had used the connection unbeknownst to him. What mattered was that the Internet subscription was in his name.

FM: This is, indeed, one of the points argued by the engineers auditioned during the discussions of the Hadopi law project: it is not possible, for users, to have the technical and material certainty that they have indeed secured their Internet connection...

JMM: Yes, I had said that too: your law project isn't going to be sustainable because you cannot ask somebody to have the technical competencies to really secure his or her Internet connection. Specialized, big companies, with important financial means, do not manage to do this. The answer I obtained was: as we live in a capitalist economy, we will create a market, and companies will find a solution. Four years later, in this economy of markets, there is no security solution that has been labeled as valid by the Hadopi authority. It looks like things are a little more complex than an ultra-liberal, capitalist vision of the Internet.

FM: After WikiLeaks, notably, the profession of investigative reporter and that of whistleblower seem to have entered a new era (Brevini et al., 2013). Have they indeed, in your opinion? I am thinking in particular about an issue that is common to journalism and scientific research – that of the investigator's relationship to her sources. How do you tackle this question in your work?

JMM: After 1999-2000, I have started writing "instructions" to secure sources, as I have briefly mentioned. I didn't need to use them that much; however, a certain amount of information, and even scoops, that I was able to obtain, I obtained them because I knew how to protect my sources: they trusted me and they knew how to contact me in a confidential and secure manner. WikiLeaks has changed the situation in two respects. First: it has revived investigative reporting, on paper mostly. Before, newspaper owners were telling us that thanks to the Internet, where everything is free, there is less and less money for newspapers. Julian Assange and WikiLeaks arrive, propose to have access to important documents, and here come the Guardian, the New York Times, mobilizing dozens of journalists for months to work with WikiLeaks and complete the investigation. Because of the Internet, investigative reporting no long-

er worked; thanks to the Internet, it has been revived again. Secondly, we have seen the rise of data journalism. Indeed, that's what happened to me: I became a journalist because I started to analyze data thanks to end-user computing capabilities, even before the label "domestic computing" existed. Here again, we witness the renaissance of investigative reporting, of whistleblowers, and I am hoping that there will be an increasing number of the latter, because our democracies are in thorough need of them.

At some point in our documentary, Assange recalls the expression of a NSA whistleblower who was explaining that we are at a "turning point", a key moment – all we need is to turn the ignition key. And if we do, we balance into a totalitarian society, because all technologies, the entire system, is in place. If Snowden hadn't done what he did, we can easily figure that in two, five, ten years, some entity would have been in the position of monitoring absolutely everything. What looked like a Hollywood legend, when "Enemy of the State" came out in theaters, is becoming more and more of a reality: today, we all have a small tracking device in our pockets – the smartphone. Traceable by intelligence agencies, traceable by the police, traceable by companies because we allowed them to do so ourselves. The dream of the Stasi, in fact! This is the importance of what Assange and Snowden have done. The former may be confined to an embassy building in London, but before that, he has fostered a global debate, and has had several important geopolitical effects, notably the Arab Spring; both of them have revolutionized journalistic practices – journalists are re-acquiring the 'fourth power' that was theirs, i.e. asking others to be accountable. The ethics of Assange and Snowden is in fact the hacker philosophy, that which was conceptualized in the early 80s in the United States: the act of hacking is an act of mobilizing for the privacy of citizens, for the transparency of institutions, for citizens' ability to control institutions rather than being controlled and manipulated by them – make it so that institutions are at our service, not the other way around (Auray, 1997; Himanen, 2001; Jesiek, 2003). This programme is at the heart of WikiLeaks, and of what it prompts journalists to do.

FM: Has anything changed in the ethics of journalism, faced with this plethora of data and sources?

JMM: I don't know if it has changed anything for journalism ethics as a whole. Myself, I have had some issues when I had to manipulate, during my collaboration with WikiLeaks, Syrian mail. I was indeed not that different from the NSA: it was, after all, millions of emails from Syrian citizens. But I haven't found much – apart from the jokes Bashar el-Assad was sending to his assistant...

Otherwise, recently, I have changed my Twitter status and I present myself as "hacker-journalist": just a few years ago, I could not have done this. Now, it is possible to qualify oneself as a hacker and nonetheless argue that you are doing good things. I still get, quite often, the question

"but then, you're a hacker, it means that you can pirate mailboxes?" – while I have done nothing illegal apart from what other investigative reporters have done: being in possession of some information I am not supposed to have. But it is my job. I follow the hacker ethos, actually, I am not quite sure of what they are being taught in journalism schools as far as ethics is concerned. Maybe, with Big Data, with yet more information at our disposal, journalism will be confronted to yet more novel ethical challenges.

What is interesting is that this situation gives more power to developers and hackers. So, there is a debate, as well, to figure out whether a hacker who goes to work for intelligence agencies lands on the "dark side of the force". Working for the NSA, is it good or is it bad? It's complicated. A priori, if one is American, it is perfectly legitimate for him to create an intelligence service that will collect information with the purpose of protecting Americans. But does this make it legitimate to spy indiscriminately on everyone?

Hacker profiles are increasingly sought after, by governments and companies at once, especially in the aftermath of Snowden. There is no doubt that this confronts the hacker to his own ethics.

FM: As you know, this interview has [initially] taken place within the frame of a dossier exploring "piracy". How is the appellation "pirate" present in the questions that interest you? What practices are associated with it – practices constrained, mobilized, "recycled" and made theirs by governments, companies, by different means such as espionage or surveillance?

JMM: For a few years, I have been teaching a course at the University of Nanterre in a department which was educating legal scholars to Internet-related issues. My mission was to increase their awareness of their practices and their very perception of the Internet. The first question I asked students was the following: "Those of you who have never pirated software, ripped a DVD, downloaded a copyright-protected mp3, please raise your hand." There was but one who did – the law enforcement officer on his continuing education stint. Nobody else. And my turn again: "Welcome to the Internet. If you don't understand this, you will not understand those who are called the "pirates" of the networks: all of us are pirates of the networks." We all are pirates, and always have been.

In 2005, the French National Assembly voted the DADVSI law, with the aim of fighting against piracy – this law was punishing the fact of hijacking DRMs[4], the restraining devices preventing the copy of digital con-

[4] Digital Rights Management (DRM) devices have the objective of controlling or limiting uses of digital works, thanks to a system of encryption and conditional access. They can be applied to different types of material devices supporting the

tent. I thought this was ludicrous: I have been a Linux user for ages, thus, my machine cannot read DRMs for which you have to go through Microsoft or Apple, thus if I wish to read a DVD which I have bought in a legitimate manner, the only way I have to do it is to pirate it. This law was making a pirate out of me, while a priori, I am a free software user, and therefore part of that small minority of people who never "pirate" software.

Thus, today, we cannot understand the Internet, the economy of sharing and access to knowledge, if we do not realize this. The totality, or near-totality of people on the Internet have at some point found themselves or put themselves in the position of violating the law, which is, after all, an unprecedented phenomenon in the history of humanity. And also peculiar is the fact that, if something is forbidden on the Internet, it reappears generally somewhere else, in some other form, some other way. Of course, we can talk again about Hadopi, who thought that to have people secure their own computers all you need to do is to "create a market".

The word "pirate" is strong – it reminds of violence, crimes, blood... and illegality. And yet, to what extent was somebody like Gutenberg harassed by authorities of the time, when typography was first introduced? Did he experience the same problems? I think that the person who says the most interesting things about this is Eben Moglen[5]. According to him, people fighting against piracy are also fighting for ignorance, illiteracy, poverty, for the interdiction of search for alternative solutions and bottom-up problem-solving: for economic interdiction against economic empowerment (Moglen, 2010). As the Internet enables so many things, the Monsantos, the Vivendis and the Sarkozys of this world interpret it as a loss of the power they still cling to. But I do not see how it would still be possible to look backwards: it will not be possible to prevent people from getting informed and from sharing, even if it involves the "piracy" of a few files – which is, by the way, often a lot simpler than buying them.

Then there is the "sexy" side of the pirate, and I think hackers have often played upon this side, the playful and adolescent one. But ultimately, I think we can make this assessment: on the Internet, each and everyone of us is a pirate – and that's good.

FM: In your opinion, what should we expect as far as evolutions of

fruition of digital works, from DVDs to tablets, and they can limit access in a variety of ways, according to geography, software, or specific reading functions.

[5] Eben Moglen is a professor of law and history of law at Columbia University, New York. He is the founder and director of the Software Freedom Law Center, which defends, *pro bono*, several actors of the free software domain, including the Free Software Foundation. His argument is that free software may be understood as a fundamental right in todays's society, due to its heavy dependence on complex technical systems. He is cited as the inspirator of the decentralized social network, Diaspora*.

surveillance are concerned, in the next few years? As U.S. President Barack Obama stated recently, is information – the ability to appropriate it, aggregate it, control it, "making sense" of and with it – the main 21st-century weapon?

JMM: In the next few years, I think we can hope for a redefinition of the legal landscape, and of what intelligence agencies may or may not do. Only Americans can decide this, despite the "pressure" put by Europe and other actors. We can also expect a redefinition, within the IETF[6] and other instances of Internet governance, of security and privacy protection norms so that there may be more privacy by design (Cavoukian, 2010), maybe even more security by design. Not only thanks to what Snowden has done, but simply because an increasing quantity of things depends on our connection to the Internet, and the fact that it is properly secured. The SCADA and a number of industrial systems are now connected via the Internet and other networks, and this may raise very important questions, because if electricity, thus connection, is cut, it will also be possible to cut off the supply of water, or other critical infrastructures. We are witnessing a militarization of the Internet, not only via surveillance, but also thanks to the so-called "offensive cyber-war", the hijacking of systems for purposes of espionage, possibly destruction.

We have been talking about the risks of cyber-war for years – I think we're fully in it right now. Assange is secluded in London, Manning will stay in jail for thirty-five years, several hackers close to Anonymous will not do without years in prison, and let us not forget Aaron Swartz's suicide, while he was facing a politico-legal machine which he did not think he could fight. On the other hand, we have a Nobel Peace Prize as the American President whose administration has launched a true "witch hunt" against whistleblowers. But my conviction remains, however, that hackers have already won. Even if we are still a minority, still mostly demonized, we have won because the general direction of History can no longer be switched – and the hacker ethos is here as it has never been before.

Acknowledgments

This interview has first appeared in French on the journal "Tracés". The complete reference to the original text is the following: Francesca Musiani (2014) '*Sur In-*

[6] The Internet Engineering Task Force (IETF) is an international and informal group (without statutes or formal membership), in principle open to every individual, but mostly composed of computer scientists and engineers. This group participates in the production of many standards that shape the Internet today, by issuing specification documents called Requests for Comments (RfCs).

ternet, on est tous pirates, et ça c'est bien.' Entretien avec Jean-Marc Manach, in "Tracés. Revue de Sciences Humaines", 26, pp. 235-247 (http://traces.revues.org/5963).

References

Aigrain, P. (2010) *Declouding Freedom: Reclaiming Servers, Services and Data, 2020 FLOSS Roadmap*, 2010 Version/3rd Edition. https://flossroadmap.coment.com/text/NUFVxf6wwK2/view/ (retrieved December 13, 2014).

Auray, N. (1997) *Ironie et solidarité dans un milieu technicisé : Les défis contre les protections dans les collectifs de hackers,* in "Raisons Pratiques", 8, pp. 177-201.

Brevini, B., Hintz, A. and McCurdy, P. (eds.) (2013) *Beyond WikiLeaks. Implications for the Future of Communication, Journalism and Society,* London, Palgrave-Macmillan.

Campbell, D. (1998) *Somebody's Listening*, in "New Statesman", 12 August, pp. 10-12.

Cavoukian, A. (2010) *Special Issue: Privacy by Design: The Next Generation in the Evolution of Privacy,* in "Identity in the Information Society", 3 (2), pp. 247-251.

Garnier, J.P., Manach, J.M., Martenot, A.N., Thorel, J. and Treguier, C. (2008) *Big Brother Awards : Les surveillants surveillés,* Paris, Zones.

Himanen, P. (2001) *L'éthique hacker et l'esprit de l'ère de l'information,* Paris, Exils.

Jesiek, B.K. (2003) *Democratizing Software: Open Source, the Hacker Ethic, and beyond*, in "First Monday", 8 (10). http://firstmonday.org/ojs/index.php/fm/article/view/1082/1002 (retrieved December 13, 2014).

Manach, J.M. (2010) *La vie privée, un problème de vieux cons?,* Limoges, FYP Editions.

Moglen, E. (2010) *Freedom In The Cloud: Software Freedom, Privacy and Security for Web 2.0 and Cloud Computing*, "Discours aux Rencontres de l'Internet Society (ISOC)", New York, February 5. http://isoc-ny.org/1338 (retrieved December 13, 2014).

Musiani, F. (2011) *Privacy as Invisibility: Pervasive Surveillance and the Privatization of Peer-to-Peer Systems*, in "tripleC", 9(2), pp. 126-140.

Musiani, F. (2013) *Nains sans géants. Architecture décentralisée et services Internet,* Paris, Presses des Mines.

Musiani, F. and Schafer, V. (2011) *Le modèle Internet en question (années 1970-2010)*, in "Flux", 85-86 (3-4), pp. 62-71.