The Impacts on the Educational Landscape ahead the Free Internet Offers, Traps and Surveillance that Threatens the Safety and Privacy on the Web.

Rogerio Roth, Ph.D.
Ca' Foscari University of Venice
Department of Environmental Sciences, Informatics and Statistics
Venice, Italy
CAPES Foundation, Ministry of Education of Brazil
posdoctor at gmail.com
rogerio.roth at unive.it

Abstract

The current educational landscape – pedagogically and technologically sound – has been undergoing several changes, mostly on what concerns the common sense in personal and institutional exposure, content and file sharing. The lack of knowledge about security and privacy besides the different ways of virtual learning environments does not guarantee a new approach or innovation. On the other hand, the adoption and effective use of fads without a previous context of experimentation, testing, protection and logic of use can bring different results of the expected negatively impacting the use of technologies to support the education.
Keywords: e-resources, oversharing, privacy, redesign, rereading, security.

1. Looking to the future: Breaking the links with the recent past.

This is not a cliché, or even the Back to the Future trilogy of science fiction adventure films written by Bob Gale and Robert Zemeckis, but to rethink education in terms of current and future technological possibilities involves experimentation, practice and feeling. Where to go? Given the diversity of scenarios and options – free or paid, open or proprietary, local or cloud, domestic or foreign – the decision-making process should take into account something more than just the omnipresent costs. Items such as security and privacy of information should be considered essential.

Many prominent people are recognized more for their eventual errors and failures than by their great achievements. It is not easy to predict the future with 100 Percent certainty. What to say when the bets are related to the future of the education area, so resilient, tough, conservative and averse to changes...

The recent past has brought us a virtual massification of academy, often without any quality or even interaction that should be mandatory in times of Web 2.0.
Regarding to the behavior on the Internet, of individuals and institutions – including educational, we witnessed the rebirth of pretentiously moderns, dazzle, boring and invasive.

“But I have everything on my plex. My diaries, my homework, my music, my books – my whole life!” (Marshall & Gaviola, 2011).

This paper is part of the results from the research “Building an Immersive Distance Learning Experience beyond Massive Open Online Courses with Web Conferencing, Socratic Method, Problem-Based Learning and Social Networks” funded by the CAPES foundation, Ministry of Education, Brazil.

Security, privacy, and responsibility are themes that consistently and recurringly are brought to the forefront – reported here to the different Internet uses.
Several universities and students do not see limits, to expose themselves (oversharing) on social networks. Likewise, it seems to lack common sense in adopting different service models offered in the cloud computing, as well as Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS) solutions such as Google Apps. Some

services apparently are free of charge, but there is always a price to pay for everything.

For many decades now, Microsoft has been criticized for its predatory monopolistic practices. Google is currently under the spotlight as well.
On the 1st April 2014 the Gmail email service (Google Mail) completed 10 years (“Gmail,” 2004), (“Gmail,” 2014). The date always refers to the celebration of April Fools' Day, sometimes called All Fools' Day – especially in Australia, Brazil, Canada, United States and Europe (“April Fools' Day,” 2013).

For Brazilians, the 1st of April has several interpretations, it also reminds the military revolution that occurred on this day in 1964 – and the harsh years that followed.
Interventions such as this are typical of the technique of a coup d'état, that the CIA has developed and applied in Brazil, artificially radicalizing the social struggles to the point of causing the imbalance in the political and destabilize governments (spooling actions), who did not submit to the strategic guidelines of the United States – who deny responsibility and complicity with the coup (plausible denial), standard by which American governments was characterized many times their intervention policies in other countries (Bandeira, 2004).

“Friday, April 3, 1964 – 12:06 p.m. Thomas Mann: I hope you're as happy about Brazil as I am. Lyndon B. Johnson: I am. I think that’s the most important thing that's happened in the hemisphere in three years. Lyndon B. Johnson: I hope they give us some credit, instead of hell.” (Beschloss, 1997).

Interpretations and historical events aside, we all (Gmail users) can be victims of this stigma. Are we fools to use the Gmail and its associated tools from Google?
What is the price we pay for the use of these “free of charge” offers?

Ribble (2014) states that, “…Gmail was not the first of its kind. In fact, it was a relative latecomer to the webmail party. Gmail's objective was not to create a totally new way of communicating, but to make radical improvements to the existing webmail model. And the last ten years leave little doubt that they've succeeded.”

They really managed to do “radical improvements”, ranging from the absurd to the unbelievable, verifiable in a judicial documentation of 30 pages, when Google acknowledged that Gmail users have no “reasonable expectation” that their communications are confidential. Its users do not have complete privacy (Rushe, 2013).
That suit, filed in May (2013), claims: “Unbeknown to millions of people, on a daily basis and for years, Google has systematically and intentionally crossed the 'creepy line' to read private email messages containing information you don't want anyone to know, and to acquire, collect, or mine valuable information from that mail.”
To John Simpson (Rushe, 2013), Consumer Watchdog's privacy project director, “Google has finally admitted they don't respect privacy”, emphasizing that, those who want some security or privacy, should not use Gmail.

The document came to light at a time when Google and other technology companies (AOL, Apple, Facebook, Microsoft, Paltalk, Skype, Yahoo and YouTube) try to explain the role they play in mass surveillance practiced by the National Security Agency (NSA) over citizens of the United States and foreigners (governments, authorities and citizens) of several friendly countries, including France, Germany, Spain and Brazil.

The denunciations of Snowden (2013), former technical expert of the Central Intelligence (CIA), occurred through the newspapers The Guardian (Greenwald, 2013) and The Washington Post (Gellman & Poitra, 2013), giving details of the information traffic carried through various surveillance programs, among them PRISM (2013) and XKeyscore (2013).
According to the information published, it is possible (XKeyscore) to read the email content of any person in the world, just knowing the email address. Any website can be verified (inbound and outbound traffic). Any computer that a person uses on the Internet can be monitored. Any

notebook can be traced – when accessing the Internet – while the user travels, to any part of the world.

Snowden (2014) said (00:03:46,445 – 00:03:59,131): “Every time you pick up the phone, dial a number, write an email, make a purchase, travel on the bus carrying a cell phone, swipe a card somewhere, you leave a trace and the government has decided that it's a good idea to collect it all, everything, even if you've never been suspected of any crime.” (“Snowden Interview,” 2014).

No new information. Snowden just proved what we all, in some way, already knew – that the control and manipulation of information have been used (by all parties) not only in times of declared war to change public opinion, to support certain actions of the rulers or even to contain the resilient and politically incorrect through the eyes of the dominant power.

If someone travels to a different country (of their usual displacements – which are monitored) and try to access Gmail through a different way than webmail immediately has the access blocked, forcing the use of a mobile phone to receive an unlock code via SMS or voice message. Google keeps a record history of the used IP addresses and suspect whenever someone gets out of their “controlled” comfort zone. Some user requested this kind of “protection” or is it possible to disable? Not... (“Basics,” 2015), (“SMS from Google,” 2015).

This kind of control – that not just Google does – seems to be meaningless for those who already transformed their life (personal/institutional) in an open book, updated and exposed 24 hours a day (Twitter/Facebook) in a sort of Big Brother (reality show).
Probably, in search of their “fifteen minutes of fame” (Warhol, 1967)...

Google or any other service provider paid or “free of charge” cannot be our PlexPad, not now; much less in the future (2149), (Terra Nova – Marshall & Gaviola, 2011).

The year 2014 was prodigal in examples of lack of privacy and security for both users and institutions, including the lack of digital literacy. The incident of August – the biggest scandal of celebrity photo leaks already occurred – exposed a security hole of the Apple's iCloud service (“2014 celebrity,” 2014).

Our lives can not be fully exposed and/or dependent on a single supplier.
That way we will be allowing connections between the various services and providing more information than necessary – both for those hosts as well as for our personal and professional contacts. Also, we are going to be hostages of a particular company – under a certain government or country – and its policies, economic interests and technological failures.

Eventually everything that goes to the cloud may be lost or even accessed by other people. If certain information is sensitive, secret or even intimate, the Internet and the vast majority of their gratis or paid services is certainly not the best place to store them. After all, nothing is forever. Google also taught us this. On Tuesday, September 30, 2014, the chronicle of a death foretold finally came true: Orkut is over (Orkut, 2014), (“Orkut Archive,” 2014).

To Assange (2014), “Unlike intelligence agencies, which eavesdrop on international telecommunications lines, the commercial surveillance complex lures billions of human beings with the promise of 'free services'. Their business model is the industrial destruction of privacy. And yet even the more strident critics of NSA surveillance do not appear to be calling for an end to Google and Facebook.”

This “business model” searches not only the destruction of privacy but also the end of anonymity and the end of freedom of opinion without reprisals.
Who should not, does not fear? Who should not, should fear yes, and with good reason...

WikiLeaks founder, Julian Assange, himself is the victim of the system, in the same way as all those who try to challenge the constructed and manipulated truths, that subsequently have become definitive and unquestionable evidences (“WikiLeaks,” 2011).

But what options are available? Fance (2013) recognizes that Gmail can be one of the most popular services, but there are many people who feel that it is far from being the best. She cites some problems and points out how the most important justification is the fact of the Google scans each email message that is sent and received. This is done so that advertisers can better target users and display ads that are more relevant to them – although from a Gmail user’s standpoint, this is considered an invasion of privacy.

If, for these reasons – or any other – someone wishes to stay away from Gmail/Google or simply wants to try something new, she lists ten major alternatives: Hushmail, Zoho, Mail.com, Outlook.com (replaced Hotmail), GMX, Facebook, Inbox.com, Yandex, Shortmail and Yahoo Mail.
There are many other options in almost every country – the Internet is a sea of possibilities – and the major players seem to have servers located in the United States, China and Russia. On Wikipedia, for example, there is an extensive compilation and comparison of providers (“webmail providers,” 2014).

Some people or institutions may want to not rely on Russian or Chinese services for several reasons. But what is the difference among staying under the surveillance of a Big Brother (Orwellian) American, Chinese, Russian, or any other controller?

This text does not intend or even has the pretense of showing anti-Russian, anti-American or anti any other country. Nothing is intended against or in favor of any party. It only reflects the absurdities to which all were thrown, implicitly or explicitly, after Second World War, during the Cold War and the ideological-political bipolarization.
What we thought we had stayed in the past seems more alive than ever.

Impossible not to relate the current ubiquitous and pervasive practices to the dystopian novel 1984 (“Nineteen Eighty-Four,” 2010) written in 1949 by Eric Arthur Blair, or rather by his pseudonym “George Orwell”. The pseudonym has always been one of the forms of anonymity.

Wilde (1891) through an assay and using a Socratic dialogue, stated that: “Life imitates art far more than art imitates life.” The Orwellian nightmare comes true.

“Sooner or later, though, you always have to wake up” (Cameron, 2009).

The anonymity nowadays is something pursued by all means and ways. On the Internet, due to the illusion that many have to be anonymous, the practice is verified even in discussion forums and/or opinion that, in a ubiquitous manner, require the use of an email of identification or affiliation to a social network – as if the two possibilities were not possible to be false and, thus, be possible to post a comment “anonymous”.

How can we distinguish current practices to those verified in the middle ages?
In a way, we live in a new “holy” inquisition, and witch hunts... Any difference even among the contemporary practices of the Gestapo, Kempeitai, NKVD, Stasi, SAVAK, KGB, MSE, FSB, OSS, DOPS, CIA, Mossad and similars?

On behalf of a anti-terror paranoia systematically fed, the “Patriot Act” (“Patriot Act,” 2008), a fascist law that invades the privacy of any American citizen (with impacts throughout the world – at airports, for example), we can not create a state of exception, trample fundamental freedoms and constitutional rights in the alleged combat against an imagined – or created intentionally – “terrorism”...

The new heretics – accused of heresy, piracy or terrorism – remain being all who are contrary to the established dogmas, those who question certain truths, considered as indisputable –

created without evidence, logic or moral use – or even those who oppose to the opinions determined by certain dominant groups. No one is discordant in itself, and any founder or participant in any practice or behaviour that may be considered divergent – in a given historical period and social reality – nothing more is than someone who, from his own point of view, believed that he was moving in the correct path. The heterodox is classified this way just because someone invested with some sort of institutional power, rated its practice or its ideas as dissonant and contrary to an official orthodoxy that if self considers as the correct path (Barros, 2008, p. 125).

There are no eternal facts, as there are no absolute truths (Nietzsche, 1908, p. 22).
Both science, law and history are made of transitional truths. There are no thorough truths in every area of human knowledge, in constantly evolving, much less in our "official story", the manipulated version of the facts that goes to the books.
After all, the paper accepts everything and who writes, defines, govern or even judges do it according to his own bias of life, including his own prejudices as well as the maintenance and commitment to the current situation.

Everyone has the right to freedom of opinion and expression?
Scientists, jurists, rulers and serious historians, exempt, uncompromised and without fear of facing the status quo and the truths imposed?
Galileo Galilei (2007) would have certainly divergent opinion about inquisitorial courts. The reality that prevails corrupts and marginalizes those who oppose the established truth, through the fear of rejection or ridicule, which makes many thinkers to remain hidden.

Many actions of certain groups which, without options, try to survive the extermination what is imposed on them and the occupation of their territories – real or virtual – are erroneously classified as "terrorists". This never can be compared with the widespread raids against civilian populations that began in Second World War and culminated with the attack with nuclear bombs on Hiroshima and Nagasaki (August 6 and 9, 1945). We have lost the moral.

The true terror remains the actions of powerful states, primitive, warlike and pre-historic imperialisms; that have not learned lessons from the mistakes of the past and insist – through a path unilaterally imagined – in denying the right to self-determination of peoples, as well as impose their vision of the world to other cultures, most of the time ignoring the cultural diversity and ethnic minorities.

On the Internet we can see that the attacks are not limited to "strategic" targets. In the case of Google actions, they are generalized. Beyond the control of the email contents we can realize an insistent and resilient way to induce and/or require the identification that matches completely to the policies adopted by this company which, often, is not shy to request additional information – another e-mail, cell phone – to connect the dots. Consequently, it became a common practice, including banks, sending codes via SMS to confirm operations, as if cell phones could not be stolen. On the contrary, mobile phones can identify the exact location of the user – or anyone who uses his phone.

Remoaldo (1998) points out that anonymity has always been an important feature of society. The need for its existence has been demonstrated over the years. It has been of great value to dissidents in countries with little or no freedom of expression, for the victims of violation and for people who might want to share their experiences without revealing their true identity. Without anonymity, these actions could result in the silencing of these people through censorship, physical aggression, loss of job, legal processes or even through murder.

Many countries allow citizens to hide their identity as part of the right to privacy, since the acts are not considered illegal. Yet even this concept of legality varies according to a particular era or social situation ("Anonymity," 2011).
Wikipedia, for example, is written collaboratively mainly by authors who use unidentifiable pseudonyms or use only their IP address, some might even use identifiable pseudonyms or

their real name (“Wikipedia: Anonymity,” 2014).

The actions of Big Brother (Orwellian) can reach everyone and the current distrust of solutions providers on the Internet entails further the desire to remain anonymous. The full anonymity on the Internet is possible but not always guaranteed, since IP addresses can be tracked and associated with a particular computer through which a message was sent or through which the contents of a website has been changed – without identifying a user directly.

Identity masking services such as Deep Web (Tor, Freenet, I2P and others like Morphmix/Tarzan, Mixminion/Mixmaster, JAP, MUTE/AntsP2P and Haystack) hinder tracing, by using technologies of distributed computing and encryption (“Deep Web,” 2008), (“Tor Project,” 2002), (“Freenet Project,” 2000), (“I2P,” 2003).
Another possibility is the use of a Virtual Private Network (“VPN,” 2013).

Hoffman (2012) says that: “All the major search engines track your search history and build profiles on you, serving different results based on your search history.” He suggests five alternative search engines for those who are tired of being tracked: DuckDuckGo, Ixquick's Startpage, Ixquick, Blekko and Ask.com/AskEraser. He also reminds us that, to surf anonymously everywhere – with slower browsing speed – the best option is the Tor browser.

The SlashGeek (“Anonymous,” 2012) recommends that not be used only the Tor (previously an acronym for The Onion Router). It indicates as the best choice to associate Tor with VPN: You-Tor-VPN or even You-VPN-Tor. Gives tips about VPNs, points out that the Google search engine should not be used and indicates the Firefox as the best browser (with the extensions Ghostery, NoScript and Adblock Plus).

A device that promises total anonymity online in a simple, non-technical and inexpensive way ($51) is the Anonabox (2012), (“Anonabox,” 2015), and there is also a free turnkey solution for application-wide online privacy. It's called Tails (“Tails,” 2009) and it is a “live” operating system, developed from the Debian (Linux) and optimized for privacy, where all network data is routed through Tor network.

Proxy servers can also be used (“Proxy,” 2010). There are different levels of proxy (web, caching, reverse, transparent, etc.) with different levels of protection and anonymity – enough to bypass the restrictions of websites even in countries where the Internet is censored or wars occur, to report the latest developments.

These technologies allow the traffic to pass through another computer before communicating with the recipient, a different user's IP address.

The Lizard Squad, group that presented itself as responsible for Christmas attacks (2014) to PlayStation Network and Xbox Live above all did so to demonstrate the incompetence of Sony and Microsoft to avoid these attacks (Pilkington, 2014).
With the attack on the Tor, anonymous Internet service, the Lizard Squad (@LizardMafia) attracted even the wrath of Anonymous (@YourAnonNews) whose only concern is the privacy made possible by the Tor, which is used by people around the world to navigate and communicate without having anyone else lurking their private activities (Smith, 2014), (Arce, 2014).

The Tor project is one of the most effective sites for encrypted communication, becoming one of the most important Internet services in the world.
Whistleblowers like Edward Snowden has used the service as well as many dissident movements and users – who are under the control of information – from countries such as China, North Korea, Cuba, Egypt, Iran, Russia and Venezuela. Without wishing to create an axis of evil, where we are free?
The Americans – and not only them – should seriously consider its use.

2. Trojan Horse

In October 2006, Google allowed educational institutions to use the Google Apps service, which is now called Google Apps for Education (“Google for Education,” 2015), formerly Google Apps Education Edition. Google Apps for Education (“Apps for Education,” 2015) is free of charge and offers the same storage space that Google Apps for Work (“Apps for Work,” 2006), formerly Google Apps for Business. Seems to be an offer they could not refuse. But, even the success stories multiply; there has not been unanimity among the universities, even among the Americans (Whittaker, 2010).

In the European Union (currently, 2015) checks are in progress to legally allow access to users' privacy and the right to be forgotten – a process that began in 2010 in Spain – as well as Google's business separation. All try curb the company's dominance in the Internet search market (Fioretti, 2014), (European Commission, 2014). Recurring issues of (lack of) privacy comes at a time when the company Google is also fighting for four years against an antitrust investigation (European Commission, 2010).

Starting in the academic year 2008/09, Ca' Foscari (UNIVE) began using Google services, starting with Gmail by shifting the MX record of domain unive.it:

```
IP address: 157.138.7.88 – Host name: unive.it
MX aspmx.l.google.com
MX alt1.aspmx.l.google.com
MX alt2.aspmx.l.google.com
MX aspmx2.googlemail.com
MX aspmx3.googlemail.com
```
source: http://network-tools.com/default.asp?prog=express&host=unive.it

This initiative is initially observed in Ca' Foscari (2008, 26) (translated): “email @stud.unive.it – Starting from the academic year 2008/09 for all students has been prepared a mail box identified by registration@stud.unive.it. The mailbox, hosted by Google, has more than 7 GB of disk space. The initiative aims to improve the quality of communications to students, and from these to the University.” Later in Ca' Foscari (2012, 55) there is a reference (translated): “It is also expected that the migration to Google Apps for Education can encounter some problems (not severe) relating to technical and/or organizational aspects” and one realizes that, even being a “free” offer from Google (without direct acquisition costs), the UNIVE paid (indirectly) for consultancy fees (translated): “Investment relating to consultancy for transition to the systems Google Apps for Education, Moodle and iTunes U.”
Both Google, Moodle and Apple do not charge (directly) the use of their platforms by universities. But one day the invoice may arrive.

Currently (academic year 2014/15), all Google Apps for Education services are available to faculty, staff, researchers (username@unive.it) and to students (registration@stud.unive.it). The authentication system of the University (translated): “To professors, employees, and researchers the email username@unive.it associated with the services Google Apps for Education; to students the email registration@stud.unive.it associated with the services Google Apps for Education;” (“autenticazione di Ateneo,” 2015): “Warning: although the new mail box is hosted by the Google operator is accessible exclusively by web address http://mail.stud.unive.it and not via www.gmail.com” (translated), (“account di posta studenti,” 2015).

However the emails are explicitly exposed on the UNIVE website, ignoring the risks involved and abstaining from using, for example, JavaScript or images.

Piotto (2014) said: “Use image instead since text email is forbidden by Italian law (legge Stanca 17/01/2004 about public administration sites accessibility). Use text like [dot] [it] or

_AT_ help spammers (see http://techie-buzz.com/featured/tips-to-tackle-email-harvesting-spam.html). Use complex system like captcha, JavaScript, etc... help us to prevent spam but block Google indexing and reduce site's usability. We are a public service, @unive.it isn't a personal email (if you want a personal email use @gmail.com), our first goal is help students and users to find us (Google indexing is necessity, not a problem), no matter if we receive spam."

This position is simply absurd, and the same can be said with respect to all the arguments offered as a reason to not protect the emails. Currently all @unive.it accounts receive a reasonable amount of spams, higher than the verified in "normal" Gmail accounts already included in lists of spammers. This is due mainly for sewing the email lists to people from academic institutions (internal and external "clients") that are made through offers sent to all account holders. I'm not referring to the absurd mailing lists (CIdE) that are created internally and, as always, shoot first, ask questions later ("Mailing List CIdE," 2015).

Why do we need an institutional email? To "prove" some affiliation?
This type of account is one which we do not have full control, which is subject to the receipt of unsolicited messages – institutional or non – originating within the institution and that, most often, we lose access to all content and contacts when we move away, or are taken away.

The UNIVE, on the flip side, provides a proxy server ("Proxy Settings," 2015), proxy.unive.it (157.138.1.34: 3128) that allows access to internal services – as if we are within the internal network, which includes email – and thus omit the location.

The security issue also calls for proper attention and information from professors to students – at all levels – in exposing and demonstrating the risks as well as suggest alternatives – not only with regard to the overexposure. Diversifying the options we will be collaborating to create a society digitally a little more safe and just.

The Russia's foreign minister, Sergei Lavrov, said at the UN that "…no one has a monopoly on truth and no one is now capable of tailoring global and regional processes to their own needs." (Lavrov, 2014). This is a correct and consistent statement – albeit absurd, coming from Russia, who practices the opposite of speech, and recurrently, in the cases of Ukraine, Georgia and Moldova.

Such a statement should even be applied to the Stalinist version of history – mostly related to the Second World War, whose events insistently have been changed and used in the wrong way (by all parties) and "Hollywood" that, in the absence of new military "victories" and in the face of repetitive failure verified later (Korea, Vietnam, Afghanistan, Iraq and Syria) does not shy to distort the facts and explore the event, apparently, to the last drop: Fury, a Sony movie (Block & Ayer, 2014).

This is not about watertight issues or problems unrelated to the entrenched reality in which many universities live. We live in a state of war, even when not declared, which includes all forms of surveillance, electronic attacks, cyber-attacks and cyber terrorism; often sponsored by governments and sovereign states – democratic or not – or by independent groups.

Angela Merkel (Germany) and Dilma Rousseff (Brazil) would have been only two, of the 35 world leaders monitored by the NSA (Rawlinson, 2013), ("Global surveillance," 2013). According to Aymone (2014), provided that the complaints have been proven many Brazilian federal public universities have adopted various new safety standards, among them the use of own email servers, something that the majority of them had already made.

Generally, there is a recommendation (DOU of 2014, October 17) so to adopt the "Guide to Good Practices on Hiring Information Technology Solutions", of the Secretary of Supervisory Information Technology of TCU (SEFTI), to decrease the risks to which IT area is subject, especially with regard to the creation of service level agreements with the applicants areas and the holding of documentation of products developed by third party companies, for that they do not become hostages of the companies contracted, who hold the knowledge of the products developed, (“Guia,” 2012).

The information leaks are not something inherent to the Internet or use of computers. It has always existed. And were not just spies of the “enemy” photographing secret documents. Most of the time it's friendly fire and the problem is at home – the leaks mostly originate from within the institutions. We slept with the “enemy” or heroes, depending on the observer's point of view...
Scanning only made things easier and faster. And the Internet allowed for greater disclosure, that is, more people have access to information.
WikiLeaks (2006) is an organization which publishes, on its website, posts from anonymous sources, documents, photos and confidential information leaked from governments or corporations, on sensitive issues.

In Russia, the Kremlin is returning to typewriters – in an attempt to avoid leaks. It has already spent nearly $15,000 on the purchase of this “modern” equipment (“Kremlin,” 2013).
The joke seems to be about to become literal also in Germany (Farivar, 2014).

Secret information must, as its name implies, be kept secret. In the case of emails, the biggest problem is what we write and for whom. Unlike spoken words (that can be recorded) emails are written and identify (digitally) the origin and destination. They can and are used as evidence, even after our own death (e.g. Steve Jobs), (Ames, 2014).

Certain words or expressions can classify any message as interesting or potentially dangerous to the eyes of the software spies who monitor the computers (locally or remotely). This is also true for all kinds of websites, including blogs and social networks. McAfee has related the search keywords more dangerous to scammers (Keats & Koshy, 2008).

A given message will be stored at least in two places: on the sender and on the receiver. Where both sides keep copies of sent and received messages on their personal equipment as well as on their servers (cloud) the same message will be, at least, in four places. That is, it is sufficient to invade or have access to only one of the options to take ownership of all content, something that not just the NSA makes with perfection.

There are several technologies to improve the security level of messages sent as the encryption and the use of certificates. But nothing is perfect. Just a password that is easy to break in order for this data to be accessed by anyone. The main thing is to use common sense in the contents and, even with respect to private messages, keep in mind that eventually the text will be accessed by others, even unauthorized, which may make different use of the information, including against us.

The issue of security, for universities, should not be restricted to emails and own servers. To Roth (2014), should be assessed what options are available free of charge at this time – and it would be both technically and pedagogically usable. The focus would not be to fall into the discussion paid vs. free, but to speak out on issues such as security and privacy. Given the current quality of free options (such as Google's package), it is an irresistible appeal to institutions, public and/or private, in lean times.

But we should not make the same mistake of the Trojans.

The end of anonymity, for example, does not mean any guarantee of the end of inappropriate content publication (Blum, 2014).

The Brazilian Civil Rights Framework for the Internet – officially Law No 12.965, of April 23, 2014 – also guarantees the freedom of expression, but registers the possibility of compensation when there is a violation of the intimacy and private life (“Civil Rights

Framework," 2014). Moody (2011) described the regulatory Framework as a law "anti-ACTA", in reference to the Anti-Counterfeiting Trade Agreement, widely criticized for restricting the freedom on the Internet and that was rejected by the European Union. Tim Berners-Lee, inventor of the World Wide Web, called it a "fantastic example of how governments can play a positive role in advancing web rights and keeping the web open" and called for other countries to follow suit of Brazil (McCarthy, 2014).

The Internet is a reflection of the imperfect world in which we live and it has its good and bad points depending on how we use it. We can observe practices that may be, at the same time, considered right or wrong, depending on who the judges (status quo). Countries such as China, North Korea and Cuba, among others, are criticized by the second largest "democracy" in the world (USA) with regard to the control what they do about Internet access.
Which country does not do the same (and not just on the Internet)?

3. Paddling against the tide

With respect to content sharing, there are conceptual differences – and distorted – as well as various interpretations about the French expression droit d'auteur (authors' rights), ("Authors' rights," 2014) and the Anglo-Saxon term copyright (right of copy), ("Copyright," 2009).

Wong (2013) compares the Chinese appropriation of western culture and the construction in the western imaginary of a China that represents the quintessential mimicry. She reveals that, the copy as learning method, common in arts academies worldwide, is part of Chinese culture and its pedagogy, linked to the thought of Confucius, to whom the copy is an exercise in humility. In 2004, responding to allegations of copyright violations, China's government argued that, thanks to the imitation skills of artists from Dafen (Shenzhen), consumers around the planet could have access to the world of great art.

This point of view can be extrapolated to music and books. But why not apply this also to education, so that more people have access?
The replication process as an instrument facilitating access to information and social change always comes up against the same issues.

Some governments insist on the way of criminalization. Projects such as the PROTECT IP Act (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act), ("PIPA," 2011) and the Stop Online Piracy Act ("SOPA," 2011) did not follow ahead. And the persecutions, the closure of some hosting services as well as the control of the search engines ("Chilling effect," 2011) have not reached the expected results, as was expected.
After all there are several other ways to share content, with greater or lesser exposure as well as the commitment of those who intend to do.
The cases of Napster, Megaupload and The Pirate Bay are exemplary. After these services have been withdrawn from the air, the options – clones or similar ones – have multiplied exponentially. In times of shared economy the solution to the "problem" does not pass by this way: prohibit, prosecute and punish...

The history has shown us that certain actions and/or positionings have different interpretations over time. We should learn more from our mistakes than from our accidental successes. There are notorious examples proving the opposite, full of discrimination of the most varied types: social class, belief, skin color, creed, disability, ethnicity, age, education, nationality, sexual orientation, political opinion, national origin, race, religion, sex or any other type. In the past, and occasionally nowadays, the discrimination was something explicit. In these politically correct times discrimination follows other models. Many people have already been barred or even lost jobs for them being exposed in social networks: their opinions, their preferences, their "friends", their followers.

The new generation are born under the illusion that there's freedom – at least on the Internet –

and there is no dominant feeling in them, of doing something wrong, with respect to the information and data sharing, whether simple personal photos as well as music, movies and books of third parties. Considering that they are the future and who controls the world is always a dated issue – we all have a life limit – this difficulty will soon be outdated.

The copy path as learning method can not be restricted to art schools (worldwide) nor be seen in a discriminatory manner as happens currently against the Chinese, in the same way as happened with the Japanese after the Second World War. Both gave us lessons that the copy process always has a cost and there always occurs some appropriation of content by who performs...

Does not fit here discuss the rights of the author or copy, but if a particular work is displayed to the public, that is, was exposed, published, rented or even sold there is no way to prevent, in practice, that people to do records (photos, audio, video, paper copies, etc.) and then display them and/or share. It is impossible and there is no Big Brother (Orwellian) that can contain this tsunami due to the omnipresence of photo and video cameras in mobile phones.
One can only try, but this is and will always be a losing battle.

4. Streisand effect

On November 21, 2014 a self-titled group “Guardians of Peace” or “GOP” would have hacked the servers of Sony Pictures, blocking all computers, blacking out the company's website, besides stealing files and leaking unpublished movies (“Sony hack,” 2014).
How a company as powerful as Sony – technologically speaking – shows itself as vulnerable to different attacks (Guardians of Peace, Lizard Squad) in so little time?

The origin of the “Guardians of Peace” is still uncertain. According to the American television channel NBC, FBI sources “investigate” if North Korea “would be” behind the attack (Williams, 2014), (“North Korea,” 2014). The Asian country has its own division of hackers within the armed forces, known as Unit 121, which is “suspected” of attacks on the United States and South Korea.

Could have been the North Koreans? Yes, in the same way that, could be the Chinese, Russians, Iranians, Japanese, Europeans, Americans (northern, central or southern), or Sony's own staff. The pseudo-defenders of freedom of expression and privacy exist everywhere.

The stronger “evidence” of the authorship of the attack would be the fact for North Korea to have a “reason” to attack the Sony Pictures: the movie “The Interview”, a bad taste comedy from Sony about the fictional assassination of the North Korean Supreme Leader, Kim Jong-un (Roger & Goldberg, 2014).

If Sony was again the victim of the enemy hidden (or declared) maybe we never have all the answers. Could have been a marketing action (internal) or the work of friendly fire (Lena), after all the repeated attacks to the Sony's structure has gotten a seemingly easy success.

All that the “Guardians of Peace” obtained in relation to threats to suspend the release of the movie was to make the even much more commented than would normally be, that is, the Streisand effect. It is an Internet phenomenon where an attempt to censor or remove any kind of information turns against the censor, resulting in the vast replication (“Streisand effect,” 2007).

It is very likely that the movie The Interview would have been unnoticed, were it not for all the controversy that surrounded it. According Chedin (2014) and Spargo (2014), there are reasons to suspect this story – which points the involvement of North Korea, or even exemption from Sony.

Through what happened Sony received disproportionate attention and the movie won an absurd free marketing. In the name of “freedom of expression” and as an act of protest and support, many people resorted to websites about cinema, notably the IMDb, and rated a perfect 10 to the movie, even before watching it (IMDb, 2014), (Savov, 2014).

They even went as far (Barack Obama) as to suggest the movie be nominated for an Oscar! (Maddocks, 2014).

The same movie that is featured in the race for the Golden Raspberry Awards (Kreps, 2015), which “honors” the worst productions of the year (2014) of American cinema.

If the movie is good or not, depends on the personal taste of each one of us.
With much good will, protest and everything else, Chedin (2014) asserts that the movie does not deserve even half of it. It is possible, but better not to rely on critics in the same way that we should not trust politicians, researchers and exempt historians.

The Sony's profits are probably being larger than “normally” would have been under standard conditions for “temperature and pressure”. Only at the premiere weekend were about $18 million, of which $15 million would be from online sales (Baker & Milliken, 2014) – the film was released simultaneously in several streaming services such as YouTube, Google Play, Xbox Videos and Kernel.

According to Sony, just in this period the movie had been purchased or rented online more than 2 million times (Baker, 2014), becomes the largest Sony Picture’s online movie of all time.

Between December 24 and January 4, this number rose to more than 4.3 million times, having raised more than $31 million from online, cable and telecoms sales. In addition, the film has earned $5 million at the theatrical box office, with 580 independent theaters showing the movie in North America (Sinha-Roy, 2015).

To what extent has Sony learned from the mistakes of the past and can be held harmless in the process? That is, put sensitive information on a server – which can be accessed via the Internet – does not refer to the rereading of an antecedent trap, in Pearl Harbor-style (“Japan Questions,” 2008) – when all the Americans aircraft carriers of the Pacific fleet had already abandoned the port, leaving only the battleships, almost all old and outdated – to achieve our true purposes?

The results, after the release of the film, has been so significant that, probably, the ports of Sony's servers will be open to the future “invasions”.
It costs much less to promote the new releases and profits online are immediate.

Any “definitive evidence” about the attack's authorship presented so far?
The government of China said that there is no evidence that North Korea is responsible for attacking the Sony Pictures, as stated by the United States (Rajagopalan & Holland, 2014).
In the past the U.S. also accused China of cyber spying, without evidence, and a U.S. official said the attack on Sony “could have used” Chinese servers to mask its origin (Wroughton & Rajagopalan, 2014).

“Could have used” is an inaccurate, partial and biased statement. Suspicion and investigate evidence is something normal. Disclose this information before to prove something is irresponsible. Call a spade a spade, with impartiality and without compromise, is another story.

The persistent and opportunistic attitude of trying to incriminate – without evidence – all those opposed to the dominant ideas of a given country does not give us the right to expose them and ridicule them (Basques, Communists, Cuban, Nationalists, National Socialists, North Koreans, Palestinians, Iranians, Ukrainians, Venezuelans, etc.).

This recurrent modus-operandi always refers to the argument used, for example, with respect to the alleged large hidden reserves of mass destruction weapons in Iraq...
The American agencies of “intelligence” CIA (Iraq) and the FBI (Sony) are so discredited that their information should always be interpreted to the contrary.
Something like the weather forecast: we would make fewer mistakes…

This is a strategy adopted by various nations, throughout history, to distort the facts, to create false truths, to obtain the support of the majority of other countries – and, sometimes, not even that.

Since the early years of the twentieth century we witness tampering, denial, creation or even the imposition of versions considered “historical” episodes as Holodomor, Katyn massacre, attack on Pearl Harbor, Holocaust, murder of John F. Kennedy, September 11 attacks, weapons of mass destruction of Saddam Hussein, Guantánamo Bay Detention Camp, etc. The list is not intended to be exhaustive nor exclusive of any country.

Conspiracy theories? Perhaps they could be considered that, but this does not mean that the huge list of evidence and proof of unofficial versions are lies (“American False Flag Operations,” 2015), (Sutton, 2001), (Sutton, 2000).

Today we think that we know what really happened in Ukraine (1932-1933), in Poland (1940), in Brazil (1964-1985) and in Iraq (2003). The history was partially rewritten – in these cases. But, many other revisions (rereadings) are required (“Holodomor,” 2010), (“Katyn,” 2004), (“Iraq,” 2003).

The official story hardly reflects the real history – what really happened – it is always distorted by the bias of one who tells – or is obliged to narrate.
We can not change the past, but we should at least try to correct our mistakes – including the “official” versions of the history – and, as far as possible, not repeat them.

Several episodes remain being victims of the manipulation of the facts nowadays. We should have evolved – as a human race – but we remain using concentration camps, performing the forced deportation of people and the extermination, practicing the most diverse types of discrimination, forcing various forms of slavery – of all colors – and exploiting the child labor.

If the year 2014 brought hope to Cuba, it also proved that this country – and not only – remains limiting and chasing the freedom of opinion.

Faced with an inert United Nations due to the limits of power and facing a “security council” that does not allow the positioning of the majority, we see the resurgence of conflicts in all continents and we are witnessing the rebirth of a new cold war in Europe.

This “security” council whose five permanent members (who have veto power) are the same as, currently, they practice the worst atrocities and crimes against humanity – without any punishment, because they consider themselves above the law that they have created for others: China (Tibet), France (Libya), Russia (Ukraine), United Kingdom (Argentina) and United States (Iraq).
In addition, we watched transfixed, the eternal victim of the Second World War (Israel) does not shirk from applying these days (with evidence) against Palestine the same crimes and persecutions which alleged that they had been victims in the past (without proof).

The battle of information – or rather, misinformation – nowadays happens mainly through the Internet. Many people who hold key positions – including presidents and prime ministers – choose to disclose relevant information via Twitter than through official statements. Nothing like creating a noise...

The truths created (lies) against Ukraine and its heroes (1942-1956) are repeated nowadays (2013-2015), (Stopfake, 2014), distorting the historical role of nationalists as Stepan Andriyovych Bandera ("Stepan Bandera," 2010) and his current followers, as well as the Ukrainian Insurgent Army ("UPA," 2007) and all tragic events that followed the Euromaidan ("Euromaidan," 2013), which began on the night of 21 November 2013 with public protests in Maidan Nezalezhnosti (Independence Square) in Kiev, demanding closer European integration. All in the hope of creating an independent Ukrainian state, and now fully integrated into the European Union.

And as in any military conflict, gives rise to the propaganda war. Given the manipulation of the news by Russian or pro-Russian agencies – many reversing totally the sense of what happens – we highlight the blog "Ukraine in Africa" ("Ucrânia em África," 2015), one of the best exempt sources of information about the absurdities that happen in this European country.

The episodes cited bring lessons in all senses of interpretation.

The year 2015 will be just another in that world powers will show their inability to resolve many major crises. The next president of the United States will have to work out if there is a middle way between the imprudences of George W. Bush and the retraction of Barack Obama. The European Union will have to decide if it wants to stick at its current borders or whether it will allow the entry of Ukraine and Turkey. The upsurge of tensions will be considered by the West as Russia's fault. Vladimir Putin, in turn, will blame the West, while encouraging Russians to turn inwards, away from the malign influence of foreigners. China should use its new leverage to push harder for a stake in global internet governance. The Big Brother (Orwellian) may become the whole world (Ahmed, Doucet, Gracie, Kendall & Mardell, 2015).

The attack occurred in France (Charlie Hebdo) on January 7, 2015 – in the event of confirming evidence that the murderers are Muslim terrorists – indirectly may introduce more difficulties Turkey, besides favoring the current racist offensive in Europe (Schofield, 2015). Probably on the day that all the much-vaunted freedoms (expression, opinion, religion and manifestation) keep distances and ethical boundaries between themselves – politically correct, and contemporary – be possible to obtain a suitable solution to all issues involving not only the complex religious world, without running the risk of messing with existing passions when it comes to faith, whatever it may be.

The history of Europe was a long blood-filled drama full of wars, conflicts, revolutions, plagues, discriminations, enforced migrations, coups and catastrophes – the majority of these events related to religion or to different visions and religious options. In name of "god" we remain watching the most resilient and regrettable episodes.
"It's not time to repeat history. It's time to make history" (#McLaren Honda).

In the same way that movie studios can get better financial results through secure online operations – lowest-cost and value to the end consumer – than in movie theaters, should universities ask themselves about the dominant model of knowledge's sale and bet on innovative online solutions (different from this e-learning low-quality model that turned massive) and with a new model of sustainability, without charging customers directly.

The OpenCourseWare have evolved into the Massive Open Online Course and the irreversible trend is to move towards full university courses, via Internet, in a safe environment and with guaranteed privacy, with certification and totally free of charge. It would not be ultimately a way unlike everyone else – a redesign – to achieve the beautiful revolutionary, democratic and constitutional standard of "universal, compulsory and free education" at all levels, to all people and without any distinction or discrimination? (Neves, 2003).

The use of free resources available on the Internet is a great asset to all universities, whether public or private, because theoretically and probably its use demand less financial resources than would be needed to develop and/or maintain services and its own structure. However, it is

necessary to moderate the enthusiasm of early adopters and dampen the skepticism with regard to novelties as well as pass on these benefits – in some way – to the users and ensure that they will have security and privacy preserved.
The destruction of privacy widens the existing power imbalance between the ruling factions and everyone else, leaving the outlook for subject peoples and oppressed classes, as Orwell wrote, still more hopeless (Assange, 2014).

In the movie Iron Man 3 (Feige & Black, 2013), Tony Stark (Robert Downey Jr.) quotes a phrase at the beginning and end of the film: “We create our own demons”...

The context is different from this paper and much closer to the Europe's strategic relationship with Russia after the end of the Cold War, but can be applied and generalized to the extent that, when we bet all our chips on a given market solution – product and/or service, proprietary technology and/or provided by a single vendor; and hosted in a single country – we became hostages of our own options, or even worse, of the third-party options to whom we entrust our information on the Internet.

References

2014 celebrity photo hack (2014, September 1). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/2014_celebrity_photo_leaks

Ahmed, K., Doucet, L., Gracie, C., Kendall, B. & Mardell, M. (2015, January 2). What will the big stories be in 2015? BBC News. Retrieved Jan 3, 2015, from http://www.bbc.com/news/world-30648444

Ames, M. (2014, March 25). Newly unsealed documents show Steve Jobs’ brutal response after getting a Google employee fired. PandoDaily. Retrieved Jan 22, 2015, from http://pando.com/2014/03/25/newly-unsealed-documents-show-steve-jobs-brutally-callous-response-after-getting-a-google-employee-fired/

Anonabox (2012, January). Retrieved Jan 22, 2015, from https://anonabox.com/

Anonabox: the Tor hardware router (2015, January 7). Retrieved Jan 22, 2015, from https://www.indiegogo.com/projects/anonabox-the-tor-hardware-router

Anonymity (2011, March 24). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Anonymity

April Fools' Day. (2013, April 4). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/April_Fools%27_Day

Arce, N. (2014, December 27). Anonymous to Lizard Squad: Keep Your Hands off Tor. Tech Times. Retrieved Jan 22, 2015, from http://www.techtimes.com/articles/23248/20141227/anonymous-to-lizard-squad-keep-your-hands-off-tor.htm

Assange, J. (2014, December 4). Who Should Own the Internet? Julian Assange on Living in a Surveillance Society. The New York Times. Retrieved Dec 16, 2014, from http://www.nytimes.com/2014/12/04/opinion/julian-assange-on-living-in-a-surveillance-society.html?_r=0

Aymone, D. (2014). Internet publication [personal communication]. Message received from <domingos.filho@unipampa.edu.br> in October 17.

Baker L. B. & Milliken, M. (2014, December 28). Sony's 'The Interview' makes $18 million in opening weekend. Reuters. Retrieved Jan 22, 2015, from http://www.reuters.com/article/2014/12/29/northkorea-cyberattack-sony-idUSL1N0UC0JO20141229

Baker L. B. (2014, December 28). 'The Interview' Becomes Sony's No. 1 Online Movie Of All Time. HuffPost. Retrieved Jan 22, 2015, from http://www.huffingtonpost.com/2014/12/28/the-interview-online_n_6388086.html

Bandeira, L. (2004). 1964: A CIA e a técnica do golpe de Estado. Revista Espaço Acadêmico, 64, ISSN 1519.6168. Retrieved Jan 22, 2015, from http://www.espacoacademico.com.br/034/34ebandeira.htm#_ftn4

Barros, A. (2008). Heresias entre os séculos XI e XV: uma revisitação das fontes e da discussão historiográfica – notas de leitura. In Arquipélago, 2 (11-12), 125-162. ISSN 0871-7664. Retrieved Dec 20, 2014, from http://hdl.handle.net/10400.3/626

Basics: Recover your account via text message (2015). Retrieved Jan 22, 2015, from https://support.google.com/accounts/answer/152124?hl=en

Beschloss, M. (1997). Taking Charge: the Johnson White House Tapes, 1963-1964. New York: Simon & Schuster, p. 306.

Block, B. (Producer), & Ayer, D. (Director). (2014). Fury [Motion Picture]. Culver City, CA, United States: Columbia Pictures

Blum, R. (2014, October 19). Proibir anonimato não impede publicação de conteúdo impróprio na Internet. Universo Online. Retrieved Dec 29, 2014, from http://noticias.uol.com.br/opiniao/coluna/2014/10/19/proibir-anonimato-nao-impede-publicacao-de-conteudo-improprio-na-Internet.htm

Brazilian Civil Rights Framework for the Internet (2014, April 23). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Brazilian_Civil_Rights_Framework_for_the_Internet

Ca' Foscari (2008). Inaugurazione 141° Anno Accademico 2008/09 Università Ca' Foscari Venezia. Retrieved Dec 10, 2014, from http://www.unive.it/nqcontent.cfm?a_id=61185

Ca' Foscari (2012, May 18). Rapporti dei Delegati del Rettore 2011. Retrieved Dec 10, 2014, from http://blogs.unive.it/users/blogrettore/weblog/09d3a/Il_lavoro_dei_delegati.html

Cameron, J. & Landau, J. (Producers), Cameron, J. (Director). (2009). Avatar [Motion Picture]. Santa Monica, CA, United States: Lightstorm Entertainment

Chedin, R. (2014, December 26). Eu vi “A Entrevista” para que você não precise. Retrieved Dec 30, 2014, from http://www.manualdousuario.net/a-entrevista-critica/

Chilling effect (2011, October 19). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Chilling_effect

Comparison of webmail providers (2014, December 6). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Comparison_of_webmail_providers

Deep Web (2008, December 27). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Deep_Web

Edward Snowden (2013, June 10). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Edward_Snowden

Euromaidan (2013, November 27). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Euromaidan

European Commission (2010, November 30). Antitrust: Commission probes allegations of antitrust violations by Google. Press release IP/10/1624. Retrieved Dec 10, 2014, from http://europa.eu/rapid/press-release_IP-10-1624_en.htm

European Commission (2014, July 3). Factsheet on the “Right to be Forgotten” rulling (C-131/12). Retrieved Dec 10, 2014, from http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

Fance, C. (2013, August 31). 10 Google Gmail Alternatives. Retrieved Dec 23, 2014, from http://www.hongkiat.com/blog/gmail-alternatives/

Farivar, C. (2014, July 14). In the name of security, German NSA committee may turn to typewriters. Ars Technica. Retrieved Jan 22, 2015, from http://arstechnica.com/tech-policy/2014/07/in-the-name-of-security-german-nsa-committee-may-turn-to-typewriters/

FBI: North Korea responsible for Sony hack (2014, December 19). NBC2 News. Retrieved Jan 22, 2015, from http://www.nbc-2.com/story/27671344/fbi-north-korea-responsible-for-sony-hack#.VKGrZsBA

Feige, K. (Producer), & Black, S. (Director). (2013). Iron Man 3 [Motion Picture]. Burbank, CA, United States: Marvel Studios & DMG Entertainment

Fioretti, J. (2014, July 24). Google under fire from regulators on EU privacy ruling. Reuters. Retrieved Dec 10, 2014, from http://www.reuters.com/article/2014/07/24/us-google-eu-privacy-idUSKBN0FT1AZ20140724

Galileo Galilei (2007, August 9). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Galileo_Galilei

Gellman, B. & Poitra, L. (2013, June 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. The Washington Post. Retrieved Dec 21, 2014, from http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-Internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Get started with Google Apps for Education (2015). Retrieved Jan 22, 2015, from https://support.google.com/a/answer/2856827

Global surveillance disclosures (2013–present) (2013, August 16). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present)

Google Apps for Work (2006, March 6). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Google_Apps_for_Work

Google for Education: Save time and stay connected (2015). Retrieved Jan 22, 2015, from https://www.google.com/edu/products/productivity-tools/

Google Launches Gmail, Free Email Service. (2004, March 30). Retrieved Jan 22, 2015, from http://searchenginewatch.com/sew/news/2065293/google-launches-gmail-free-email-service

Greenwald, G. (2013, June 6). NSA collecting phone records of millions of Verizon customers daily. The Guardian. Retrieved Dec 21, 2014, from http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Guia de boas práticas em contratação de soluções de tecnologia da informação (2012). Retrieved Jan 22, 2015, from http://portal2.tcu.gov.br/portal/pls/portal/docs/2511467.PDF

History of American False Flag Operations (2015). 9-11 Review. Retrieved Jan 22, 2015, from http://www.911review.com/articles/anon/false_flag_perations.html

History of Gmail. (2014, December 3). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/History_of_Gmail

Hoffman, C. (2012, May 9). 5 Alternative Search Engines That Respect Your Privacy. How-To Geek. Retrieved Jan 4, 2015, from http://www.howtogeek.com/113513/5-alternative-search-engines-that-respect-your-privacy/

Holodomor (2010, November 6). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Holodomor

How to be completely Anonymous online (2012, June 15). Retrieved Jan 22, 2015, from http://www.slashgeek.net/2012/06/15/how-to-be-completely-anonymous-online

I2P Anonymous Network (2003). Retrieved Jan 22, 2015, from https://geti2p.net/en/

Il sistema di autenticazione di Ateneo (2015). Retrieved Jan 22, 2015, from http://www.unive.it/nqcontent.cfm?a_id=156283

Informazioni account di posta studenti (2015). Retrieved Jan 22, 2015, from http://www.unive.it/nqcontent.cfm?a_id=55452

Iraq War (2003, March 20). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Iraq_War

Japan Questions 9/11 and the Global War on Terror (2008, February 2). The Straight Dope - Fighting Ignorance Since 1973. Retrieved Jan 22, 2015, from http://boards.straightdope.com/sdmb/showthread.php?t=490675

Katyn massacre (2004, December 16). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Katyn_massacre

Keats, S. & Koshy, E. (2008). The Web’s Most Dangerous Search Terms. McAfee, Inc. Retrieved Jan 22, 2015, from http://promos.mcafee.com/en-US/PDF/most_dangerous_searchterm_us.pdf

Kremlin security agency to buy typewriters 'to avoid leaks' (2013, July 12). BBC News. Retrieved Jan 22, 2015, from http://www.bbc.com/news/world-europe-23282308

Kreps, D. (2015, January 5). 'The Interview,' 'Sex Tape' Lead Razzies' Worst Film Shortlist. Rolling Stone. Retrieved Jan 22, 2015, from http://www.rollingstone.com/movies/news/interview-sex-tape-razzies-worst-film-shortlist-20150105

Lavrov, S. (2014, October 15). No One Has A Monopoly On Truth. Sergey Lavrov's U.N. Address. Retrieved Jan 22, 2015, from http://www.informationclearinghouse.info/article39972.htm

Maddocks, P. (2014, December 26). Obama says 'The Interview' should be in Oscar conversation. Seacoast Online. Retrieved Jan 22, 2015, from http://www.seacoastonline.com/article/20141226/News/141229425

Mailing List CIdE (2015). Retrieved Jan 22, 2015, from http://virgo.unive.it/cide/?page_id=1728

Marshall, B. (Writer), & Gaviola, K. (Director). (2011, December 12). Within [Television series episode]. In Spielberg, S., Braga, B., & Ovitz, M. (Producers), Terra Nova. Los Angeles, CA: 20th Century Fox Television. Retrieved Oct 20, 2014, from http://www.springfieldspringfield.co.uk/view_episode_scripts.php?tv-show=terra-nova&episode=s01e11

McCarthy, K. (2014, April 23). Brazilian president signs Internet civil rights law. The Register. Retrieved Dec 30, 2014, from http://www.theregister.co.uk/2014/04/23/new_bill_signed_in_brazil_guaranteeing_civil_rights_on_internet/

McDougall, P. (2010). Exclusive: Gmail Ditched By Major University. Dark Reading: Connecting the Information Security Community, May 5. Retrieved Oct 17, 2014, from http://www.darkreading.com/risk-management/exclusive-gmail-ditched-by-major-university/d/d-id/1088833?

Moody, G. (2011, October 4). Brazil Drafts An 'Anti-ACTA': A Civil Rights-Based Framework For The Internet. Techdirt. Retrieved Dec 30, 2014, from https://www.techdirt.com/articles/20111004/04402516196/brazil-drafts-anti-acta-civil-rights-based-framework-Internet.shtml

Neves, F. S. (2003, November 29). Propinas, ensino superior público, a razão dos estudantes e a falta dela. Retrieved Nov 30, 2011, from http://a_verdade_da_mentira.weblog.com.pt/arquivo/040197.html

Nietzsche, F. (1908). Human, all too human; a book for free spirits. Chicago: C. H. Kerr. Retrieved Dec 20, 2014, from http://hdl.handle.net/2027/mdp.39015003747733

Nineteen Eighty-Four (2010, March 25). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Nineteen_Eighty-Four

Orkut (2014, september 30). Retrieved Sep 30, 2014, from https://www.orkut.com/

Orkut Community Archive (2014, October 1). Retrieved Jan 22, 2015, from http://orkut.google.com/

Pilkington, E. (2014, December 25). PlayStation and Xbox facing issues after Christmas Day attack. The Guardian. Retrieved Jan 22, 2015, from http://www.theguardian.com/technology/2014/dec/25/playstation-xbox-down-lizard-squad-hack-christmas

Piotto, A. (2014). Internet publication [personal communication]. Message received from <piotto@unive.it> in April 23.

PRISM (2013, July 4). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/PRISM_%28surveillance_program%29

PROTECT IP Act (2011, May 12). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/PROTECT_IP_Act

Proxy server (2010, August 14). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Proxy_server

Proxy Settings Instructions (2015). Retrieved Jan 22, 2015, from http://www.unive.it/nqcontent.cfm?a_id=164714

Rajagopalan, M. & Holland, S. (2014, December 22). China condemns cyberattacks, but says no proof North Korea hacked Sony. Reuters. Retrieved Dec 30, 2014, from http://www.reuters.com/article/2014/12/22/us-sony-cybersecurity-idUSKBN0K006U20141222

Rawlinson, K. (2013, October 26). NSA surveillance: Merkel's phone may have been monitored 'for over 10 years'. The Guardian. Retrieved Jan 22, 2015, from http://www.theguardian.com/world/2013/oct/26/nsa-surveillance-brazil-germany-un-resolution

Receiving an SMS from Google (2015). Retrieved Jan 22, 2015, from https://support.google.com/accounts/answer/3367674?hl=en

Remoaldo, L. (1998). O anonimato na Internet: um direito ou uma ameaça? UP. Retrieved Dec 23, 2014, from http://paginas.fe.up.pt/~mgi97018/is/anoni.html

Ribble, J. (2014, March 31). Happy 10th Birthday, Gmail! Marketing Cloud. Retrieved Dec 20, 2014, from http://www.exacttarget.com/blog/happy-10th-birthday-gmail/

Rogen, S. (Producer), & Goldberg, E. (Director). (2014). The Interview [Motion Picture]. Culver City, CA, United States: Columbia Pictures

Roth, R. (2014). Technology Integration at a Crossroads: Dead End Street or New Horizons? TOJDEL, 2 (4), 112-140. ISSN 2147-6454. Retrieved Oct 17, 2014, from http://www.tojdel.net/volume.php?volume=2&issue=4

Rushe, D. (2013, August 15). Google: don't expect privacy when sending to Gmail. The Guardian. Retrieved Dec 19, 2014, from http://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit

Savov, V. (2014, December 22). The internet decides that The Interview is a perfect movie. The Verge. Retrieved Jan 22, 2015, from http://www.theverge.com/2014/12/22/7433229/the-internet-decides-that-the-interview-is-a-perfect-movie

Schofield, H. (2015, January 7). Charlie Hebdo: Gun attack on French magazine kills 12. BBC News. Retrieved Jan 22, 2015, from http://www.bbc.com/news/world-europe-30710883

Sinha-Roy, P. (2015, January 6). Sony's 'The Interview' earns $31 million online, $5 million at theaters. Reuters. Retrieved Jan 22, 2015, from http://www.reuters.com/article/2015/01/06/us-northkorea-cyberattack-sony-idUSKBN0KF23L20150106

Smith, D. (2014, December 26). Anonymous To 'Lizard Squad': Stop Attacking Tor. Business Insider. Retrieved Jan 22, 2015, from http://www.businessinsider.com/anonymous-to-lizard-squad-stop-attacking-tor-2014-12

Snowden Interview NDR English (2014, January 26). Retrieved Jan 22, 2015, from https://archive.org/details/SnowdenInterviewNDREnglish

Snowden, E. (2014, January 26). Interview by H. Seipel. Edward Snowden exklusiv – Das Interview [Television broadcast]. Moscow: Norddeutscher Rundfunk. Retrieved Dec 21, 2014, from http://www.liveleak.com/view?i=f1d_1390839693

Sony Pictures Entertainment hack (2014, November 21). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Sony_Pictures_Entertainment_hack

Spargo, C. (2014, December 25). North Korea was NOT behind the Sony hack according to multiple security experts who discredit FBI findings and reveal that a studio insider named 'Lena' may be responsible. Daily Mail. Retrieved Dec 30, 2014, from http://www.dailymail.co.uk/news/article-2887081/North-Korea-NOT-Sony-hack-according-multiple-security-experts-discredit-FBI-findings-reveal-insider-named-Lena-responsible.html

Stepan Andriyovych Bandera (2010, January 22). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Stepan_Bandera

Stop Online Piracy Act (2011, October 26). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Stop_Online_Piracy_Act

Stopfake.org (2014, March 2). Retrieved Jan 22, 2015, from http://www.stopfake.org/en/news

Streisand effect (2007, June 15). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Streisand_effect

Sutton, A. C. (2000). Wall Street and the Rise of Hitler. Studies in Reformed Theology. Retrieved Jan 22, 2015, from http://reformed-theology.org/html/books/wall_street/index.html

Sutton, A. C. (2001). Wall Street and the Bolshevik Revolution. Studies in Reformed Theology. Retrieved Jan 22, 2015, from http://reformed-theology.org/html/books/bolshevik_revolution/index.html

The Freenet Project (2000, March). Retrieved Jan 22, 2015, from https://freenetproject.org/

The Interview (2014). The Internet Movie Database (IMDb). Retrieved Jan 22, 2015, from http://www.imdb.com/title/tt2788710/

Tor Project: Anonymity Online (2002, September 20). Retrieved Jan 22, 2015, from https://www.torproject.org/

Ucrânia em África (2015). Retrieved Jan 22, 2015, from http://ucrania-mozambique.blogspot.com/

Ukrainian Insurgent Army (2007, December 18). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Ukrainian_Insurgent_Army

Virtual private network (2013, February 2). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Virtual_private_network

Warhol, A. (1967, October 13). Sculpture: Master of the Monumentalists. Time, 90, 80-86. Retrieved Dec 24, 2014, from http://content.time.com/time/magazine/article/0,9171,837402,00.html

Whittaker, Z. (2010, May 7). UC Davis scraps Gmail pilot: Privacy levels “unacceptable”. ZDNet, iGeneration. ZDNet. Retrieved Dec 23, 2014, from http://www.zdnet.com/article/uc-davis-scraps-gmail-pilot-privacy-levels-unacceptable/

WikiLeaks (2006, December). Retrieved Jan 22, 2015, from https://wikileaks.org/

WikiLeaks: Secrets and Lies. (2011, November 30). Retrieved Jan 22, 2015, from https://wikileaks.org/Guardian-s-WikiLeaks-Secrets-and.html

Wikipedia: Anonymity (2014, December 11). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/Wikipedia:Anonymity

Wilde, O. (1891). The Decay of Lying: An Observation. London: Oneworld Classics. Retrieved Dec 20, 2014, from http://www.online-literature.com/wilde/1307/

Williams, P. (2014, December 18). North Korea Behind Sony Hack: U.S. Officials. NBC News. Retrieved Jan 22, 2015, from http://www.nbcnews.com/storyline/sony-hack/north-korea-behind-sony-hack-u-s-officials-n270451

Wong W. (2013). Van Gogh on Demand: China and the Readymade. Chicago: University of Chicago Press. 320 p. ISBN: 0-226-02489-X

Wroughton, L. & Rajagopalan M. (2014, December 23). Internet outage seen in N. Korea amid U.S. hacking dispute. Reuters. Retrieved Jan 22, 2015, from http://in.reuters.com/article/2014/12/22/china-usa-cybersecurity-idINKBN0K004G20141222

XKeyscore (2013, July 31). Retrieved Jan 22, 2015, from http://en.wikipedia.org/wiki/XKeyscore