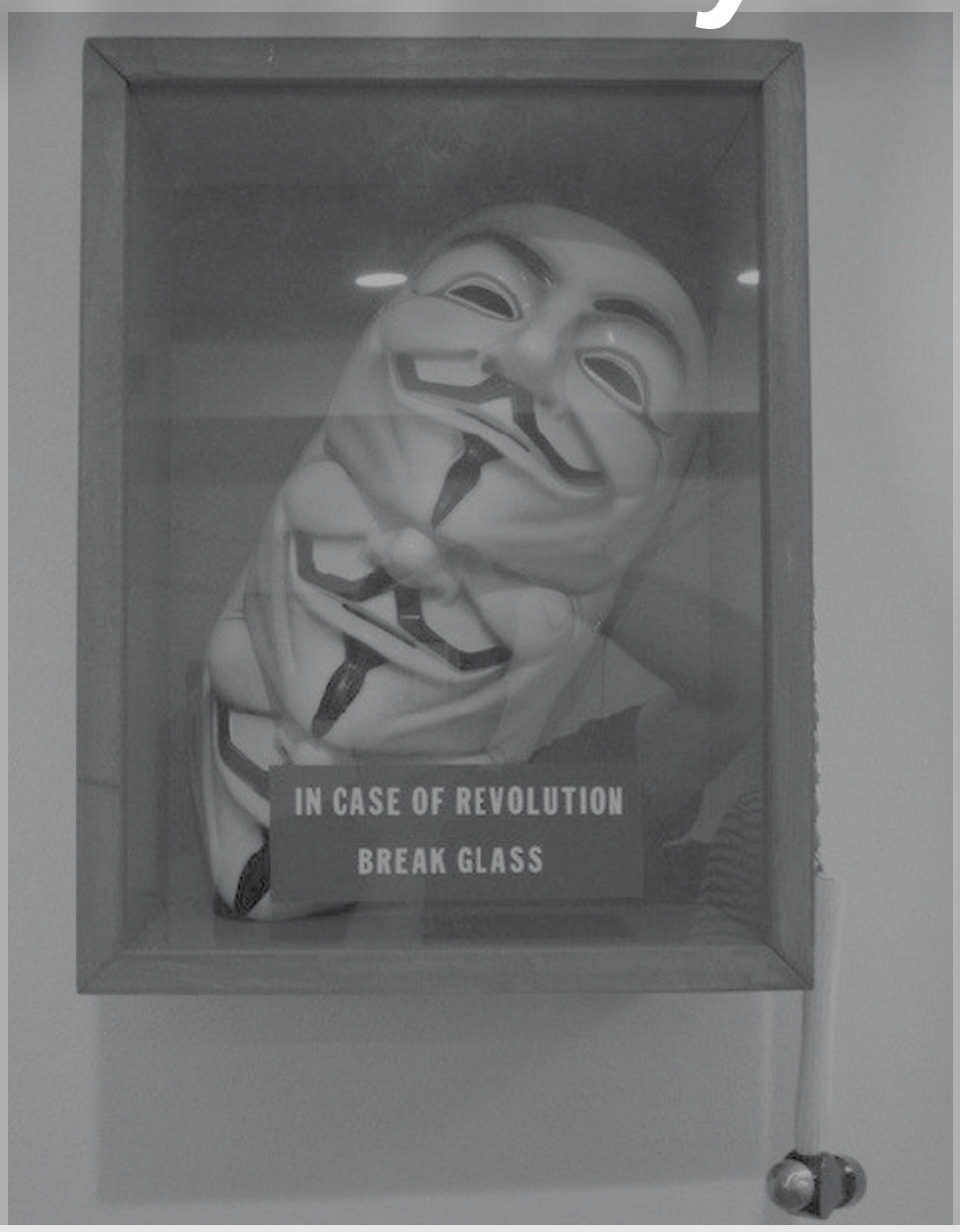
Piracy, Privacy
and the *Wiki Way of Web*



Keeping it Private

Privacy is about having more control over the personal information that we have disclosed. As we disclose more information online, we must ask who might access it and why.

By Nishant Shah

As a researcher of the blink-and-change cyberspaces, I am often asked about the future of all things digital. I generally refuse to answer such questions because researchers are happier talking about things past than things present. Also, when people ask questions of the future, they are more interested in gadgets and platforms. Will Facebook survive the next year? Will more people use Twitter? Is the mobile the new weapon of protest? Shall we all soon talk only on FaceTime? I shrug my shoulders at these questions. However private information and privacy ties all these questions.

I pronounce that 2012 is going to be the year of Personal Information Management and the need for increased privacy, where more than anything else, people will realise that what they do online is not only significant to their present, but that it might bite them in their digital futures. We have heard stories that have hinted at management of information and reputations online. Young people put compromising pictures and videos online, severely damaging their social and professional relationships; people express opinions on public forums, which might not necessarily reflect them well; users reveal personal information, which can be abused by those with malice. These instances should remind us that unlike in the physical worlds, where our foot-in-the-mouth moments, youthful indiscretions or embarrassing behaviour quickly runs through the grapevine and is forgotten, in the digital worlds, the things that we say and do, stay long after we have forgotten them.

And this is where privacy kicks in. Many people in India, when they encounter the idea of "privacy", raise their eyebrows. Culturally, we are not very private people. We celebrate our triumphs and sorrows in public, freely part with information to strangers on train rides, and don't have qualms asking about age, marital status or salary. In the age of ubiquitous computing, we must remember that once something has been committed to the online world, it will be etched somewhere and will be available for somebody else to look at. The internet, specially with increasing bandwidth, expanded spectrum and cloud-based distributed data storage, is an unforgiving space that never lets go.

Privacy, in this brave new world, is not about disclosure. It is becoming increasingly clear that we will need to disclose more and more of our private information if we want services — from government public delivery systems to private credit and education — online. However, once we have disclosed our private information, then what? Who uses it? Who reads it? Who stores it for what purpose? What are the implications of having that private information out there?

In the digital world, privacy is about having more control over the personal information that we have disclosed, the right to know who, where, when, how and for what purposes information that we have willingly disclosed is used. And as the country finalises privacy bills, this right of the individual, whose private information is going to feed government and business ecologies, is at stake.

There is a need to institute better regulation around data protection, data mining, data retention and data retrieval that is still in the limbo in our country, at the mercy of privately crafted terms of service that we blindly accept while signing into the digital world.

It is time to move away from understanding privacy as disclosure to privacy as control of information — to know who is doing what with your private information and how you should have a say in it. And it is time to realise that just because you don't have anything to hide, does not mean that you need to be in a state of disclosure. There is a reason why you have curtains in your house, or do not allow strangers to look into your bags.

QUOTE

It is time to move away from understanding privacy as disclosure to privacy as control of information.

Originally published in Indian Express edition 15 January 2012.

twitter

Emily Goodhand @copyrightgirl 26 Jan
Copies equivalent to counterfeits? RT @CopyrightReport Software #**piracy** costs California over $1 billion in lost wages bit.ly/xqjj4a

haroldfeld @haroldfeld 26 Jan
'That new 3D printing is the very Devil, I tells ya! It will mean **piracy**! Panic I says!' bit.ly/AnOqJy (via @joemillerjd)

Laws alone won't put a lid on piracy

Aqeel Qureshi @Aqeel_Qureshi 10m
The EU and 22 member states sign the controversial ACTA 'Internet surveillance' treaty textually.org/tv/archives/20... via @textually

albertmuc Albert Mucunguzi
RT @todaysocial: FBI seeks app to monitor social media ow.ly/8l9fl
1 minute ago

scl feed @computersandlaw 2h
Google's Privacy Counsel Peter Fleischer on the right to be forgotten: goo.gl/tN0dR
Retweeted by PrivacyMatters

Tariq Khokhar @tkb 24 Jan
"**Open Data**" Needs to Die? (the term, not the stuff!) j.mp/xO5x4c #opendata

The Next Web @TheNextWeb 5h
The FBI will look to seize **Megaupload**'s user data in its entirety this week tnw.to/1Czdz by @jonrussell on @TNWinsider

glynmoody Glyn Moody
MegaUpload Alternatives See Surge In Traffic After Shutdown - bit.ly/wdMbjp well, what did they expect?
7 minutes ago

ISO @isostandards 2h
Digital age: Are we experiencing transparency or the end of privacy? Standards for security & privacy can prevent the latter #RSWEF #WEF

Tim O'Reilly @timoreilly 24 Jan
Shakespeare and Beethoven would both have been subject to takedown under today's corrupted copyright laws oreil.ly/yfEUhh #SOPA/#PIPA

Mikko Hypponen @mikko 4h
Hey @Skype, do you guys have any idea how the US authorities gained access to the Skype chat logs between **Megaupload** employees?

Forbes.com Tech News @ForbesTech 28 Jan
Twitter Users Call for **Blackout** to Protest Censorship bit.ly/AzxsP2

Anonymous @AnonymousPress 17h
Users of #**Megaupload** who legally stored their data on the site are suing the US government for data theft. bit.ly/xWK4wS #ReTweet!

Howard Rheingold @hrheingold 29 Jan
8 million Wikipedia users looked up their congressional reps; 4.5 million signed Google's petition to stop SOPA lat.ms/A7VEA2

Wired @wired 8h
One upside of software **piracy**: the preservation of software history. bit.ly/z9ZyYY

Emily Turrettini @textually 9m
Twitter can now censor tweets on a country by country basis while keeping it available in the rest of the world bbc.co.uk/news/world-us-...

Guardian Tech @guardiantech 5m
Angry Birds boss: '**Piracy** may not be a bad thing: it can get us more business' bit.ly/y7yKQA

HarvardKennedySchool @Kennedy_School 25 Jan
RT @shorensteinctr: Vivek Kundra: **Open data** via networks shift power from corporations to individuals hvrd.me/wtkStH

Face / Off: Should any Internet freedom ever be sacrificed to fight piracy?

Summary: SOPA-like legislation wasn't the right way to fight piracy. But won't a better solution still require some compromises?

Lawrence Dignan

Decidedly Yes or A Resounding No

Opening Statements

Zack Whittaker

It isn't the Wild West anymore

Larry Dignan: The Internet has grown up with this somewhat ludicrous idea that there's this heavy dose of freedom and anything goes. The reality is that every entity that plays on the Internet---advertisers, content providers, information producers, service providers and the U.S. government---all have a role in tracking what you do and roles to thwart piracy. The Internet just isn't Wild West anymore although some folks like to portray it that way. If we want professional content and capital risk, we have to fight piracy. This argument also goes beyond Hollywood and the music industry. Pirated software costs technology giants a bundle too. Will that anti-piracy movement mean that some freedom falls away? Yes, for people who are pirates/criminals. Criminals sacrifice freedom in real life. Is the Internet all that different?

For me, the question about whether Internet freedom can ever be sacrificed for piracy is decidedly yes. We just have to be smart about who loses the freedom.

We would not stand for it

Zack Whittaker: The answer of course is simply a resounding "no". As seen in recent weeks with the SOPA and PIPA protests, the Web would become a stagnating pool of offline sites and 404 messages.

Pandora's box was opened with peer-to-peer file-sharing during the late '90's. Nothing was done at the time, and now our respective governments are trying to claw back what little control it has on Web users' actions.

We as a society have seen what a "free and open" Web is---something the founding fathers of the Internet prescribed---and it would be inconceivable to see a fragmented, distorted and 'broken' online world.

Simply put, we would not stand for it. We can only really miss something once it has gone, and as seen with recent protests, a significant minority speaking on the vast majority would not let such infringed freedoms happen.

If it started with piracy, it would never stop.

// The biggest change between the 20th century and the 21st is that all of the gatekeepers are going away. For the first million years or so of humanity, information was incredibly scarce, and it was an incredibly powerful thing that people devoted their entire lives to uncovering... but somewhere around 1997 it changed, and we moved from famine to glut.

I read somewhere that there were more books published in a week than there were published in all of 1950, or something like that. Is that a good thing? I'm not sure. It makes it harder to find the things that you like... It's now the job of the crowd and the hive mind to do that.

I think people in Hollywood are convinced that people would suddenly start buying DVDs again if only they could stop all this peer-to-peer file sharing and so on. They just are fundamentally missing the point... genies don't go back in bottles once they're out

Neil Gaiman, English author of short fiction, novels, comic books, graphic novels, audio theatre and films

NEWS

Sorting Out the Sharing License Shambles

At the heart of the various movements based around sharing -- free software, open content, open access etc. -- lie specially drawn-up licenses that grant permissions beyond the minimal ones of copyright.

http://www.techdirt.com/articles/20120110/07201317364/sorting-out-sharing-license-shambles.shtml

Supreme Court says police need warrant for GPS tracking

Justices decide firmly for privacy in their first ruling on government use of digital technology to monitor people.

http://articles.latimes.com/2012/jan/24/nation/la-na-court-gps-20120124

Google updates policy to track users across all of its services

The Internet search giant's move, which will cover services that include email, Web search and YouTube, could invite heavier scrutiny of its privacy practices.

http://articles.latimes.com/2012/jan/25/business/la-fi-google-20120125

Do You Like Online Privacy? You May Be a Terrorist

A flyer designed by the FBI and the Department of Justice to promote suspicious activity reporting in internet cafes lists basic tools used for online privacy as potential signs of terrorist activity. The document, part of a program called "Communities Against Terrorism", lists the use of "anonymizers, portals, or other means to shield IP address" as a sign that a person could be engaged in or supporting terrorist activity.

http://publicintelligence.net/do-you-like-online-privacy-you-may-be-a-terrorist

Nilofar Shamim Ansher

"Is sharing stealing?"

Like · · Follow Post · January 27 at 12:03pm

Philip Que-Sell I have a pretty eclectic view on this as you know. It's stealing, when you use copyrighted content to enrich yourself, may that be economical or to burst your identity. I mean this especially with respect to the music label I run with my friends. Since our content is easy accesible via the web, and ~3€ for a release of 3 tunes is not expensive, it is stealing when russian rippers put our releases on their blog or 10-cent/download sites.

January 27 at 12:08pm · Like

Simeon Oriko I don't think its stealing Philip Que-Sell. Honestly, I think copyright is way too slow in keeping up with recent digital cultures and trends.

January 27 at 12:10pm · Like

Philip Que-Sell I agree with you to some point Simeon. Yet thters ed to be re-thought: stealing as well as copyright.

January 27 at 12:12pm · Like

Philip Que-Sell ^ ^ the terms need to be re-thought

January 27 at 12:13pm · Like

Maureen Agena So what's the use of having it on the web if one does not want it shared? Best thing to do is keep it to oneself. How are you defining "Stealing" here? Is it the acual plagarism? What if I "share" and acknowledge soures, is that also be "Stealing" oh voluntarily helping the author/owner to spread their message?

January 27 at 12:32pm · Like · 1

Nishant Shah Nilofar Shamim Ansher I think Simeon's idea was good... to have it as a thread here. And then maybe we can scrape it for the newsletter? I have many things to say on this, but might be more interested in a dialogue :)

January 27 at 12:37pm · Like · 2

Nishant Shah Let me just throw in a provocation nonetheless - Sharing is stealing if you are sharing something that does not belong to you. That is obvious when you look at physical property. Robin Hood, no matter what his noble intentions, is definitely still stealing. However, what is at stake is the nature of property and possession online, which might help us reformulate the question. Because when you share something digital, without hurting the person's right to own the original or the original object, then of course there is no stealing. And hence, what gets invoked is the regime of licensing and IPR regimes.

January 27 at 12:40pm · Like · 1

Philip Que-Sell Maureen Agena - - it seems like you refer to a different example, than the one I mentioned. If so I totally agree with you. Like if someone shares my poem/ academic work, because s/he likes it, that's totally cool. Yet, if a small label and a musician put work into a release, the situation is way different. One could argue that 3€ might be way to high for global contexts in whioch this is like the salary of a month. Then we, as a label, would need some digital retail solution which can adjust the retail price according to location. I think my friends would agree with me on this point. The main question remains: Is it legitimate to use a product made by someone just like you, who doesn't wanna play the big corporate game?

January 27 at 12:41pm · Like · 1

Simeon Oriko Firstly, I cosign every single word Maureen Agena says.

January 27 at 12:42pm · Like

Simeon Oriko Secondly, Nishant Shah, stealing implies wrongful possession, not sharing...unless you want to say all those that benefited from Robin Hood's theft were thieves as well.

January 27 at 12:44pm · Like · 1

Philip Que-Sell When reading myself, I realize that there are huge differences. I, as a normal German citizen, am in a pretty good position to be productive, even though I'm a broke student. So if someone from not a 'western developed' context rips my music in order to enjoy it, because s/he simply couldn't afford it. I'd be 100% fine with it. What just really pisses us (the label) off, is the fact that people who have the resources rip our music. And that is not right. And by not right, I am referring to a philosophical discourse strongly influenced by idealism/humanism.

January 27 at 12:46pm · Like · 1

Nishant Shah Simeon Oriko there is also an accessory to crime. So even an unknowing person in possession of stolen goods is liable for prosecution. But that is not the point I was making. I was saying that in the whole construction of 'sharing-stealing' argument, ownership is often glossed over. The rights of sharing are linked to the rights of possession, the way I understand it - You share what you own. When you share something that belongs to somebody else, even if it is not for your personal gain, is still stealing. Hence, rhetoric around whether sharing is stealing needs to be exploded to ask questions about, whether, within the digital systems, ownership is absolute!

January 27 at 12:50pm · Like

Philip Que-Sell Nishant Shah, how can there be no personal gain if you share some something that doesn't belong to you. There is always a personal gain. Mostly one in the realms of identity. The most important question in my eyes is rather: is the product an accessory, or is it important for the Common?

January 27 at 12:55pm · Like · 2

Philip Que-Sell And, Nishant Shah, I think ownership can never be absolute. Not even in the material world. It remains always relative. Isn't it exactly the relation between good and its producer that gets blurred or lost in the web?

January 27 at 12:58pm · Like

Simeon Oriko Spot on question Nishant. Hence my thought that copyright is too slow. Not sure if this is a good idea but what if copyleft (e.g. creative commons) was the default standard in the digital domain as copyright is outside of it? All it would require is attributing shared material. If copyright was to be seriously enforced in the digital domain, how much of an uphill task would it be if you compared? I think we need to have the end in mind and not just the process. (Last statement vaguely reminds me of a discussion either at the thinkathon or in Jo'burg)

January 27 at 12:59pm · Like

Samuel Tettner This discussion is great! 19 comments so far...I signed one of these petitions that Google had on the blackout date, and my congressman in the US sent me the following email. Notice how he says that sharing files is "China stealing jobs from the US":

January 27 at 1:32pm · Like

Samuel Tettner https://docs.google.com/document/d/1GQeslkVT3Jes1AIQAJGQj6UkaMfXhTZwJ39IHVaGnKs/edit

January 27 at 1:32pm · Like

Samuel Tettner Do you guys think Rubio has any idea what he is talking about?

January 27 at 1:40pm · Like

Nilofar Shamim Ansher Can promotion/publicity of a material be interchangeably used with sharing of the same? YouTube has a profit-making policy where, if you have certain number of subscribers signing up to your channel you get paid. So, if I simply upload a host of Hollywood videos and get enough people to subscribe, then I am making money out of "property" that I have no ownership over. Does this strike as unethical? Also, there is no mention about the technology itself that makes such "sharing" routine, e.g. YouTube, Facebook and Twitter make their money / business model is based on the idea that people online want to share and that it is normal / routine to do so.

January 27 at 1:43pm · Like

Nilofar Shamim Ansher Samuel: Rubio's campaign / staff writer needs to brush up his PR skills :)

January 27 at 1:44pm · Like

Frank Odongkara The problem with copyright when it points to digital material is complicated. Consider these scenarios.

1.I store a music file I purchased on a server and give users the ability to only stream it from my blog.
2.I store a music file I purchased on a server and give users the ability to download; intentionally or not.

The first case is stealing if the purchase agreement doesn't allow public use of content. If however I pay a fee that allows me to display content to the public then I am not stealing e.g cinemas.

The second case is stealing if I do not have a license/ agreement to resell/distribute; a very rare scenario of the thousands of websites that provide these services. This case is also same as ripping or copying a file from one computer to another.

The problem however is with the producers as I see it. They should be able to come up with a technology that doesn't support copying of material. However much we want to love to download illegal free stuff, we got to admit that we are stealing.

January 28 at 2:55am · Like · 2

Philip Que-Sell So you want DRM back Frank? I think that'll always be cracked.

January 28 at 12:11pm · Like

Frank Odongkara It could solve a lot of problems. It sure can be cracked but then they've got to keep ahead and keep improving security issues.

January 28 at 1:09pm · Like

Philip Que-Sell Hehe. Good way to keep/make jobs Frank. But what I really don't like about DRMs is that I, as end-user, will most likely have difficulties copying my downloaded songs onto my different players. I'd rather be for the open web solution, where there are no restrictions. People just should get aware of the fact that if you rip music from a small label, you kill it and thereby your chance to get the stuff you like in the future. Just as a reminder, I'm solely talking about goods as accessories. If we have an example where the good is used to improve the knowledge of society, I want it to be as free as possible.

January 28 at 1:23pm · Like

Philip Que-Sell Like how should I deal with the scenario in which I need to analyze a film for school? Do I need to purchase/rent the film, ror shouldn't it be in the database of my school's library?

January 28 at 1:24pm · Like · 1

Simeon Oriko www.extremetech.com/computing/114493-why-i-pirate valid argument in my assessment.

January 28 at 5:45pm via mobile · Like

Nilofar Shamim Ansher If I wasn't intending to buy a DVD in the first place — if I don't have the money to buy the DVD, for example — what is the impact of me downloading an XviD rip? There isn't one. - VERY interesting point from Simeon Oriko's article :)

January 28 at 6:40pm · Like · 1

Nilofar Shamim Ansher Philip For academic work, your institution should ideally support you with the material. But for most of us, consumption is not neatly bracketed into an identifiable purpose. I might just want to browse through a scholarly article and not really review it - equivalent to flipping through a new magazine in a supermarket and then putting it back on the shelf - I wouldn't want to pay for such academic works. However, scholars and institutions argue that they have put years into that research and should be compensated for it. It really all boils down to m.o.n.e.y.

January 28 at 6:44pm · Like

Nilofar Shamim Ansher One of the comments beneath Simeon Oriko's article makes a fine distinction between copying and sharing. When you share something, there is just one original copy and that same original is passed around, but when it comes to sharing online, multiple copies are made of the original. In real life, if the prices were right and no music was available online for download, I would actually go to a store and buy a CD. I guess, we need to reframe the idea of business, property and IP rights taking into consideration the newer technologies that have burst on to the creative scene since 1980s, beginning wt the walkman! January 28 at 6:54pm · Like

Nikhil Pahwa As a content creator, how do i monetize? I either monetize by selling copies of that work, or by showcasing advertising around the work. When it gets shared, it loses the ability to monetize and pay the content creator. Many blogs that have republished our content @medianama have argued that they provided a link back. The link back doesn't do anything for us.

The other key change that has taken place over the last couple of years is the advent of applications which change the form factor - like pulse, flipboard and zite. They claim that they are like RSS readers, and do not monetize, but like RSS readers, the publisher doesn't monetize the eyeballs. So, what do we do? As you said, it does boil down to money and while the cost of distribution has been disrupted by the Internet, the cost of content creation (people) and marketing is comparatively higher.

I did a straw poll on twitter yesterday, asking people to identify Independent Indian digital publications doing high quality content with a substantive audience. In response, didn't even get a list of 10. Makes me wonder sometimes why I'm in this business, because I want someone to come and compete, push us to do better. Dont want to get too comfortable, cause it's all downhill from there.

January 29 at 6:25am · Like

Andrés E. Azpúrua I ment to post it here but couldn't find the thread:

To watermark or not to watermark:
¿What to do when there are 10 pages of sites using your photograph?

My experience and personal conflict around abuse of my photography while also wanting people to use and reuse it.

http://tumblr.andresazp.com/post/16783453845/to-watermark-or-not-to-watermark-que-hacer

Tuesday at 2:49am · Like

Nilofar Shamim Ansher Andrés E. Azpúrua what does the blog say? give us a summary please? O_O

Yesterday at 2:50pm · Like

http://player.vimeo.com/video/29996808?portrait=0

To watermark or not to watermark:

¿Qué hacer cuando hay 10 páginas de Google llenas de sitios que usan tu foto?

Eso me pregunto luego de probar la búsqueda por imágenes con la que es probablemente mi foto más exitosa.

Algunas dan creditos y otras son completamente descaradas usando fotos de otros en sus páginas comerciales. Otras son blogs de tumblr que dan referencias al "original" en Flickr, y a esas personas les agradezco infinitamente su aprecio y respeto.

Pero si mi foto ya está en laxa licencia Creative Commons Atributiva-No Comercial-Compartelgual y deseo que se comparta bajo estas condiciones el dilema queda en cómo evitar su abuso, pues las marcas de agua limitan el potencial de reutilización y en consecuencia su valor como un producto cultural, por eso las evito.

Como vieron, al menos por ahora, le coloqué una ligera marca de agua y un mensaje en la esquina hasta que termine de aceptar la pérdida o concluya que la imagen sin marcas vale más que el riesgo de sufrir lo considero como abuso.
by Andres Azpurua

Science and Censorship: A Duel Lasting Centuries

William J Broad

The specter of censorship loomed over science last week with news that a federal advisory panel had asked two leading journals to withhold details of experiments out of fear that terrorists could use the information to make deadly flu viruses — the first time the government had interceded this way in biomedical research.

But science and secrecy go back centuries, their conflicting agendas often rooted in issues of war and advanced weaponry. Self-censorship — the kind of confidentiality being requested of the two journals, Science and Nature — was even mentioned by Bacon, the 17th-century British philosopher long credited with illuminating the scientific method.

Governments have repeatedly tried to keep scientific information secret in fields as diverse as math and cryptography, physics and nuclear science, optics and biology. Now the call for concealment is falling on one of the hottest of contemporary fields — virology, where researchers are tinkering with the fundamentals of life to better understand whether altered flu germs might set off deadly epidemics.

"It's a story with mythological resonance," said Steven Aftergood, director of the project on government secrecy at the Federation of American Scientists and the publisher of Secrecy News, an e-mail newsletter. "It reflects the view that knowledge is power and some kinds of knowledge have destructive power."

A lesson of history, Mr. Aftergood added, is that censorship often fails because science by nature is inherently open and gossipy — all the more so today because of instant communication and international travel.

"The notion that the boundaries of knowledge are defined by what is published by Science and Nature is quaint," he said, referring to the journals. "For better or worse, the way that knowledge is disseminated today is ever less dependent on the flagship journals. It's done by global scientific collaboration, draft papers, online publication, informal distribution of preprints, and on and on."

The most famous case of scientific suppression remains that of Galileo, who in 1633 was forced by the Roman Catholic Church to disavow his finding that the Earth revolves around the Sun. But over the centuries, the big clashes between science and the authorities came to center on highly destructive arms.

Starting in 1943, work in the United States on atom and hydrogen bombs led to a sprawling system of classification that in time involved millions of people and billions of dollars in security precautions. It was a world of safes and barbed wire, where individuals voluntarily gave up their rights of free speech.

In 1953, Julius and Ethel Rosenberg were executed after being convicted of passing bomb secrets to Moscow.

But atomic lore kept leaking. Today, nine nations have nuclear weapons, and dozens more are said to possess the secretive information, the technical skills and — in some cases — the materials needed to make them.

A new field came under scrutiny in the mid-1970s, when Washington tried to clamp down on publications in cryptography — the creating and breaking of coded messages. A breakthrough threatened to make it easer for the public to encrypt messages and harder for federal intelligence agencies to decipher them.

Agents of the National Security Agency — an organization so secret its initials were jokingly said to mean No Such Agency — paid a visit to Martin Hellman, an electrical engineer at Stanford University. "They said, 'If you continue talking about this, you're going to cause grave harm to national security,' " he recalled.

Eventually, the government gave up, and the cryptography advances grew into a thriving global industry.

Article Copyright The New York Times. Read the article here: http://www.nytimes.com/2011/12/27/science/science-and-censorship-a-duel-lasting-centuries.html?_r=2&ref=science

Why I pirate...

Your [game/book/movie/song] is too expensive

Justifications

By Sebastian Anthony

Without getting mired down in the subjectivity of "expensive," I merely mean that I should get more for my money. When I pay $12 to watch a movie at the cinema, should I really be forced to watch through 20 minutes of commercials and 15 minutes of movie trailers? When I pay $60 for a video game, do you really have the right to stop me from reselling the game? The definition of "buying" seems to change on a monthly basis.

Most importantly, though, when I buy an album from iTunes, why does it cost $9.99, and why does only 94 cents of that goes to the artist? With boxed, shelved albums I can almost see the logic — distribution and shelf space costs a lot — but why does the publisher get a full $5.35 per digital album sale, really? The same problem is rife on Steam, where digital copies usually cost more than the meatspace version from Amazon.

At this point you usually hear the argument that publishers and broadcasters spend a lot of risky money on new artists, and thus deserve a bigger cut — but in a day and age where indie developers are creating games like Minecraft (and making millions), and superstars like Justin Bieber are discovered on YouTube, I don't really buy it.

There's another very different side to the "your X is too expensive" argument, too: Namely, digital goods generally have the same price all over the world. A friend of mine in Malaysia once said to me: "Seb, I can either buy the latest Elder Scrolls game, or I can feed myself for more than a month." This isn't an easy problem to overcome — if games were $5 in Malaysia, there would be a huge gray market of cheap, imported games — but it does further elucidate the issue of overpriced digital media.

That is why I pirate:

Because digital games, movies, and music are overpriced and don't kick enough money back to the original artist.

When you strip away the FUD and flowery prose from my pro-piracy justifications, though, it all ultimately comes down to money — and indeed, one of the strongest counterarguments against piracy is "if you can't afford it, don't buy it." If you don't want to spend $10 on the latest Katy Perry album, then simply do without it. You don't have to pirate that game; you don't have some kind of innate privilege that compels you to download it. Put simply, I pirate because I can, but that doesn't mean I should.

On the flip side of that, though, who actually loses something when I pirate a digital version of a game? The RIAA, MPAA, and others continue to spin piracy as theft, but we know that's not true: I'm not taking my game from anyone. It's not like Little Timmy arrives home to find out that he can't play Lego Star Wars because Sebastian has stolen the grubby disc. If I wasn't intending to buy a DVD in the first place — if I don't have the money to buy the DVD, for example — what is the impact of me downloading an XviD rip? There isn't one.

Furthermore, it has been repeatedly shown that pirates actually spend more money on music, movies, and games than non-pirates — because, as it turns out, pirates are usually superfans that want to want to watch every movie, play every game, and listen to every B-side track created by their favorite artist. In other words, they might pirate a lot — which harms no one, remember — but they also fork over much more money to publishers, distributors, and broadcasters than their peers.

When it comes right down to it, the only real argument against piracy is that you are depriving the artist — the game studio, the writer, the musician — of compensation for his work. As it stands, the only real way around this is to support independent artists, where all or most of your money goes directly to the creator. Unfortunately, though, it isn't indie artists that write the laws: That privilege belongs to Big Media with its armada of lawyers, lobbyists, and incredibly deep pockets.

Why do you pirate?

Read the blog online: http://www.extremetech.com/computing/114493-why-i-pirate/2

The right to be forgotten, or how to edit your history

By Peter Fleischer

The "Right to be Forgotten" is a very successful political slogan. Like all successful political slogans, it is like a Rorschach test. People can see in it what they want. The debate would sound quite different if the slogan were actually something more descriptive, for example, the "right to delete". The European Commission has now proposed to make the "right to be forgotten" into a law. It's a big step to turn a vague political slogan into a law. The time for vague slogans must now give way to a more practical discussion of how the "right to be forgotten" could actually work.

What is the "right to be forgotten"? There is a spectrum of views. On one end of the spectrum, the "right to be forgotten" is simply viewed as a re-branding of long-standing data protection principles, in particular: the rights to access and rectify one's own personal data, the right to oppose processing of one's personal data in the absence of legitimate purposes, the principle of data minimization. On this end of the spectrum, people think that the "right to be forgotten" is nothing new; at most, it is simply an attempt to apply long-standing data protection principles to the new worlds of the Internet and modern technologies. I'm firmly in this school of thought.

On the other end of the spectrum, the "right to be forgotten" is viewed more sweepingly as a new right to delete information about oneself, even if published by a third-party, even if the publication was legitimate and the content was true. This school of thought believes that people should have the right to force third-parties to delete content about them (photos, blogs, anything) that violates their sense of privacy, which in practice usually means their online reputations. Common examples of things people want to remove are compromising photos, references to past criminal matters, negative comments, etc. While I strongly believe that people should have the right to complain to third-party websites about information that is published there about them, I am deeply skeptical that the laws should obligate such third-parties to delete information on request of data subjects.

This raises troubling questions of freedom of expression.

There is an even more extreme end of the "right to be forgotten" spectrum, which holds that this deletion right can be exercized not just against the publisher of the content (e.g., a newspaper website), but even against hosting platforms and other intermediaries like search engines that merely host or link to this third-party content. This view is being litigated in Spain, as the Spanish Data Protection Authority is suing Google to delete links to third-party content, like newspaper articles, that the DPA has acknowledged are legal. In other words, the DPA is attempting to apply this reading of the "right to be forgotten" to delete links to content in a search engine, despite the fact that the original content is legal and will remain on the Web. Cases like this will require judicial review, since they clearly posit a conflict of two fundamental rights: privacy and the "right to be forgotten" against freedom of expression. I expect this issue to be considered at the European Court of Justice.

As this debate unfolds, the lack of clarity is raising false expectations. As people read that there will soon be a legal "right to be forgotten", they are asking DPAs and search engines to delete third-party content about themselves or links to such content. I regularly hear requests from people to "remove all references to me, Mrs. X, from the Internet". No law can or should provide such a right, and politicians and DPAs should not mis-lead them to expect it.

We need more public debate about what the "right to be forgotten" should mean. We also need a debate about how it should be applied to hosting platforms and search engines. I think a balanced and reasonable and implementable approach is possible, based on a few principles: 1) people should have the rights to access, rectify, delete or move the data they publish online. 2) people should not have the automatic right to delete what other people publish about them, since privacy rights cannot be deemed to trump freedom of expression, recognizing that some mechanisms need to be streamlined to resolve these conflicts. 3) web intermediaries host or find content, but they don't create or review it, and intermediaries shouldn't be used as tools to censor the web. Stay tuned, and Happy Data Protection Day.

Read the article online: http://peterfleischer.blogspot.com/2012/01/right-to-be-forgotten-or-how-to-edit.html

Why History Needs Software Piracy

How copy protection and app stores could deny future generations their cultural legacy.

By Benj Edwards

Amid the debate surrounding controversial anti-piracy legislation such as SOPA and PIPA, our public discourse on piracy tends to focus on the present or the near future. When jobs and revenues are potentially at stake, we become understandably concerned about who is (or isn't) harmed by piracy today.

I'm here to offer a different perspective, at least when it comes to software piracy. While the unauthorized duplication of software no doubt causes some financial losses in the short term, the picture looks a bit different if you take a step back. When viewed in a historical context, the benefits of software piracy far outweigh its short-term costs. If you care about the history of technology, in fact, you should be thankful that people copy software without permission.

It may seem counterintuitive, but piracy has actually saved more software than it has destroyed. Already, pirates have spared tens of thousands of programs from extinction, proving themselves the unintentional stewards of our digital culture.

Software pirates promote data survival through ubiquity and media independence. Like an ant that works as part of a larger system it doesn't understand, the selfish action of each digital pirate, when taken in aggregate, has created a vast web of redundant data that ensures many digital works will live on.

Piracy's preserving effect, while little known, is actually nothing new. Through the centuries, the tablets, scrolls, and books that people copied most often and distributed most widely survived to the present. Libraries everywhere would be devoid of Homer, Beowulf, and even The Bible without unauthorized duplication.

The main difference between then and now is that software decays in a matter of years rather than a matter of centuries, turning preservation through duplication into an illegal act. And that's a serious problem: thousands of pieces of culturally important digital works are vanishing into thin air as we speak.

The Case of the Disappearing Software

The crux of the disappearing software problem, at present, lies with the stubborn impermanence of magnetic media. Floppy disks, which were once used as the medium du jour for personal computers, have a decidedly finite lifespan: estimates for the data retention abilities of a floppy range anywhere from one year to 30 years under optimal conditions.

A floppy stores data in the form of magnetic charges on a specially treated plastic disc. Over time, the charges representing data weaken to the point that floppy drives can't read them anymore. At that point, the contents of the disk are effectively lost.

This becomes particularly troubling when we consider that publishers began releasing software on floppy disk over 30 years ago. Most of those disks are now unreadable, and the software stored on them has become garbled beyond repair. If you've been meaning to back up those old floppies in your attic, I have bad news: it's probably too late.

To make matters worse, software publishers spent countless man-hours in the 1980s preventing us from archiving their work. To discourage piracy, they devised schemes to forever lock their software onto a single, authorized diskette. One popular copy protection method involved placing an intentionally corrupt block of data on a disk to choke up error-checking copy routines. It worked so well that it also prevented honest attempts to back-up legally purchased software.

If these copy protection schemes had been foolproof, as intended, and copyright law had been obeyed, most of the programs published on those fading disks would now be gone forever. Many cultural touchstones of a generation would have become extinct due to greed over media control.

> IF COPY PROTECTION SCHEMES HAD BEEN FOOLPROOF, AND COPYRIGHT LAW HAD BEEN OBEYED, MOST OF THESE PROGRAMS WOULD NOW BE GONE FOREVER.

It's not just floppy disks that are under threat. Thousands of games published on ROM cartridges and as enormous arcade cabinets are now hard to find and can only run on electronic hardware that will eventually degrade beyond repair. Publishers have re-released a handful of the most prominent games among them on newer platforms, but the large majority of legacy video games don't get this treatment. Pirates liberate the data from these ROM chips and allow them to be played, through software emulation, on newer consoles and PCs.

Pirating also makes foreign game libraries easily available for historians to study. Some games only appeared on writable cartridges in Japan via download methods like the Nintendo Power flash cart system and the BS-X Satellaview. Those would be entirely out of the reach of Western historians today without previous efforts to back them up illegally.

For a sample slice of what's at stake when it comes to vanishing software, let's take a look at the video game industry. The Web's largest computer and video game database, MobyGames, holds records of about 60,000 games at present. Roughly 23,000 of those titles were originally released on computer systems that used floppy disks or cassette tapes as their primary storage or distribution medium.

23,000 games! If game publishers and copyright law had their way, almost all of those games would be wiped from the face of the earth by media decay over the next 10 years. Many would already be lost.

For the past decade, collectors and archivists have been compiling vast collections of out-of-print software for vintage machines (think Apple II, Commodore 64, and the like) and trading them through file sharing services and on "abandonware" websites. Through this process, they've created an underground software library that, despite its relative newness, feels like the lost archives of an ancient digital civilization.

As a journalist and historian, I rely on these collections of pirated software to do my job. I'd rather it not be that way, but there is no legal alternative (more on that in a moment).

The compilation of this underground library–a necessary resource for future historians–is a brave act of civil disobedience that needs to continue if we are to protect our digital heritage. As we'll see, the greatest threats to software history lie not behind us, but directly ahead of us.

Why Preserve Software?

Before we go any further, let's take a step back and consider why we should preserve software in the first place. Software often seems inconsequential because of its ephemeral nature. It's a dynamic expression of electrons on a computer screen, and that doesn't mean much, instinctively, to brains that evolved to recognize value in physical objects.

But software is also a powerful tool whose mastery says something profound about our civilization. If we look back through a museum, we can get a good idea about a certain society's potential by examining its tools. If a civilization could build threshing machines, for example, we know that they could harvest and process wheat much faster than people 100 years earlier. That, in turn, might explain a known population boom.

Read the article online: http://technologizer.com/2012/01/23/why-history-needs-software-piracy/

Laws alone won't put a lid on piracy: Silos across the world of content

By Melissa Bell

On Amazon, a book titled "Horror Stories" offers some tantalizing reads: "The Tell-Tale Heart," "The Purloined Letter," "The Monkey's Paw." For any fright fan, the stories are beloved spine-tinglers of the best sort and, judging by the front cover, the work of one Maria Cruz.

The book went on sale in November, but it is already out of print. It's hard to imagine that anyone associated with the actual authors — Edgar Allan Poe and W.W. Jacobs — pocketed any profits.

The self-published book was just one of hundreds of plagiarized books that New York University journalism professor Adam L. Penenberg discovered on the site after an author tipped him off two weeks ago to the rampant practice.

Penenberg traced one of the books to an online forum where Internet scammers sell marketing plans solely for this purpose. "Want to create Kindle books in 15 minutes or less? … I don't write a thing. I just create the covers and upload. Then I move on to the next book," one ad reads.

Penenberg, a technology author, has found his own books being shared illegally online. "They copy and paste the material and send it out. It's pure profit. Money rolls in whether you're doing anything or not," he said in a phone interview from his New York home.

Earlier this month, a battle between Internet companies and Hollywood studios ground to a halt when Congress effectively tabled anti-piracy legislation. The detractors called the laws overreaching and vague. Proponents, many of whom hold copyrights, called the laws necessary to battling the piracy problem. Although the debate is on hold, as the "Horror Stories" example shows, a workable solution remains elusive.

A recent study released by Envisional, an online security firm, reports that almost a quarter of all the bandwidth used in the world is carrying unauthorized material. The United States is the most law-abiding country in the world when it comes to Internet piracy, the study found. Material moving legally from Netflix accounts for 29 percent of American Internet usage.

About the same percentage of European users use BitTorrent, which can be used for illegal sharing of copyrighted material. Part of the problem is that content that is available legally in one country may not be in another.

Those divisions, says Julie Samuels, an Electronic Frontier Foundation staff attorney, contribute to piracy. "It's really troubling how we see silos across the world of content … instead of a truly international community of content."

For example, when Megaupload, a file-sharing site accused of copyright infringement, was shut down last week, a friend in Belgium wondered on Facebook how he would keep up with "30 Rock" now. "If they offered me a way to buy it, I would," he wrote.

Samuels echoes my friend's frustration. She says corporations do not recognize that "consumers will pay for content when they can get it how they want it."

The solution needs to be a combination of smart legislation and more forward-thinking corporate initiatives. "You're not going to be able to train six-to-seven billion people around the world to respect copyright," Penenberg said.

Article copyright Washington Post. Read the article online: http://www.washingtonpost.com/lifestyle/style/online-piracy-hasnt-gone-away/2012/01/25/gIQAMEsnVQ_story.html

Why 2012, despite privacy fears, isn't like Orwell's 1984

Last week was a remarkable one for the Web: A week that proved George Orwell's "Nineteen Eighty-Four" incredibly prescient yet woefully incorrect.

The online world is indeed allowing our every move to be tracked, while at the same time providing a counterweight to the emergence of Big Brother.

Nike last week announced the upcoming launch of the Nike FuelBand, a wristband that tracks your physical exercise and creates a "FuelScore" of your activity level. This score can optionally be shared with your friends on Twitter and Facebook.

Or how about the Fitbit Aria? Announced this month, this Internet-connected scale tracks your weight and provides the option to share it with friends on the Web.

These devices are part of a growing trend that tech watchers have labeled both "personal analytics" and "quantified self." The concept: Self-improvement becomes easier when you're able to track your own activities. Increasingly, consumers are tracking their every move and posting this data online.

Unlike in Orwell's dystopian world, however, people today are making a conscious choice to do so.

Or how about Facebook's new features? On Wednesday, the social networking site announced an expansion of its "Open Graph," allowing users to share more of what they do online automatically. Rather than hitting a button to share something, Facebook's Open Graph requires the user to authenticate an application only once. After that, it'll share everything you do on the application by default.

Among the activities Facebook wants you to share: Your travel plans, what you're eating, what you're cooking, what you're drinking (thanks to a wine app), what you're buying, the videos you're watching, the books you're reading, your location and more.

If this sounds invasive, remember that users choose to share all this information. Increasingly, it seems there's a demand for services that share every facet of your life. The difference between this reality and Orwell's vision -- outlined in his chilling 1949 novel -- is the issue of control: While his Thought Police tracked you without permission, some consumers are now comfortable with sharing their every move online.

The past week's events also upturned Orwellian predictions of centralized power. Opponents of SOPA, a proposed anti-piracy bill, seeded a grass-roots uprising on social networks. This culminated in the temporary shutdown of Wikipedia, Reddit and other websites last Wednesday.

The aim: To demonstrate how untenable these user-generated websites would be if SOPA were passed. The online protest was extremely effective: On Friday, the chief sponsor of SOPA pulled the bill "until there is wider agreement on a solution."

The world of 2012 is both reminiscent of Orwell's vision and radically at odds with it. Connected lifestyles are creating a world in which sharing your activities may become the norm, albeit through choice and not coercion. And yet this connected society is also empowering people in new ways, providing a counterweight to big business and big government.

While Orwell correctly predicted that technological advances would let authorities track our lives, he failed to predict the inverse: That we would use these new technologies to keep an eye on them, too.

Article copyright CNN.com. Read the article online: http://articles.cnn.com/2012-01-23/tech/tech_social-media_web-1984-orwell-cashmore_1_online-protest-sopa-share?_s=PM:TECH

Our next issue focuses on youth-led citizen action movements in the Global South.

It might be something as revolutionary as the Arab Spring or something grounded in the grassroots, as Uganda's 'Walk to Work', or how about the wildly popular Facebook group that championed the cause of women to be able to drive in Saudi Arabia? Some victorious, many silent, and still others that were headline grabbing like the OWS movement across the major cities of the world. Share with us stories from your region.

Editors: Philip Ketzel *philip.ketzel@googlemail.com* and Nilofar Ansher *nilofar.ansh@gmail.com*

Get in touch with us for submission details.

Research

The dual nature of wikipedia understood through ANT

Samuel Tettner, October 2011

Wikipedia is an interesting phenomenon for those in the STS community who like to study knowledge and how it is produced in society. This is because Wikipedia seems to have a contradicting identity; on one hand Wikipedia is perceived as the embodiment of a new paradigm in knowledge production. As Wikipedia co-founder Larry Sanger claimed in 2007, Wikipedia represents "the democratization of knowledge itself, on a global scale, something possible for the first time in human history. Wikipedia allows everyone equal authority in stating what is known about any given topic. Their new politics of knowledge is deeply, passionately egalitarian" (Sanger 2007). On the other hand, the kind of knowledge that Wikipedia is concerned with helping produce could be qualified as "scientistic" – that is to say a kind of knowledge divorced form the socio-cultural and political content where it was produced. This conception of knowledge as "neutral" is outdated and at times dangerous[1]. Wikipedia is caught in a conflicting perception; at the same time at the forefront of how the internet is allowing anyone to produce knowledge, yet applying a definition of said knowledge which is in contradiction to the very nature of how it was produced. This article uses the notion of "scripts" borrowed from the Actor-Network Theory to try and understand this how this apparent identity dichotomy arises and how it has benefited Wikipedia so far.

http://tettner.com/post/11117114038/the-dual-nature-of-wikipedia-understood-through-ant

Randoms in my bedroom: Negotiating privacy and unsolicited contact on social network sites

Robards, B. (2010) "Randoms in my Bedroom: Unsolicited contact on social network sites", Prism, 7(3): http://www.prismjournal.org/fileadmin/Social_media/Robards.pdf

The immense popularity of social network sites such as MySpace and Facebook has caused a significant shift in the way social interactions occur on the internet. Online interaction is no longer the sole domain of people seeking contact but rather it has become a key medium for maintaining and strengthening social relationships. This article draws on empirical research investigating emerging social practices being developed by young Australian internet users on social network sites. Consistent with other current research, this article argues that social network sites are increasingly regarded as private spaces where young people are 'hanging out' and articulating or playing with notions of identity and belonging. Some social networks have even been likened to bedrooms for teenagers, or are arguably replacing shopping centres and parks as spaces for casual youth interaction. Based on empirical research, this article tests these metaphors and suggests measures to strengthen their validity. As multiple social relationships are collapsed under the banner of Friendship on social network sites, important issues about privacy and audience management need to be addressed. What constitutes 'Friendship' in the Facebook era? How do young people deal with unsolicited contact in these private spaces? This article argues that young users of social network sites on the Gold Coast in Australia are, consistent with research being conducted throughout the world, developing increasingly complex strategies for managing their online privacy and social interactions.

Sociology, New Media, Communications, and Youth

"But the data is already public": on the ethics of research in Facebook

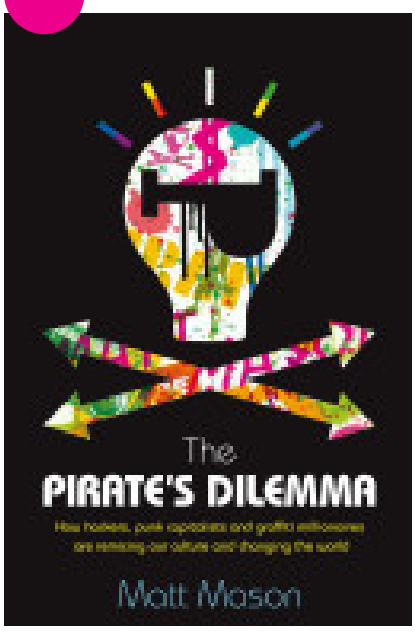
Michael Zimmer, 4 June 2010

http://uwm.academia.edu/MichaelZimmer/Papers/915786/_But_the_data_is_already_public_on_the_ethics_of_research_in_Facebook

Abstract: In 2008, a group of researchers publicly released profile data collected from the Facebook accounts of an entire cohort of college students from a US university. While good-faith attempts were made to hide the identity of the institution and protect the privacy of the data subjects, the source of the data was quickly identified, placing the privacy of the students at risk. Using this incident as a case study, this paper articulates a set of ethical concerns that must be addressed before embarking on future research in social networking sites, including the nature of consent, properly identifying and respecting expectations of privacy on social networking sites, strategies for data anonymization prior to public release, and the relative expertise of institutional review boards when confronted with research projects based on data gleaned from social media.

Keywords: research ethics, social networks, facebook, privacy, anonymity

Editor Recommends



Book:
The Pirate's Dilemma:

How Hackers, Punk Capitalists, Graffiti Millionaires and Other Youth Movements are Remixing Our Culture and Changing Our World

The Pirate's Dilemma tells the stories of youth culture uncovering, for the first time, what it is that transforms underground scenes into global industries. Matt Mason, successful entrepreneur, argues that that from youth `culture, out on the edges of the mainstream, come the ideas that ultimately change the mainstream itself – whether it's graffiti, piracy, hacking, open source culture or remixing. In the course of doing so he unravels some of our most basic assumptions about business and society and pinpoints trends to look out for in our future. Because right now, everyone, from the ceo of a mainstream company to a teenager wanting to start the next youth culture revolution, is struggling with a new dilemma: that we can all – companies and individuals alike – be pirates now. And as piracy increasingly changes the way we find, use and sell information, how should we respond? Do we fight pirates, or do we learn from them? Should piracy be treated as a problem, or a whole new solution?

Penguin Books Ltd, 01-May-2008

Book:
Free Culture:

The Nature and Future of Creativity

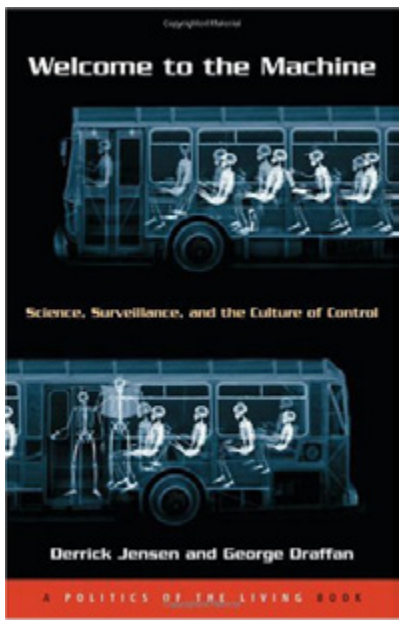
Lawrence Lessig, "the most important thinker on intellectual property in the Internet era" (The New Yorker), masterfully argues that never before in human history has the power to control creative progress been so concentrated in the hands of the powerful few, the so-called Big Media. Never before have the cultural powers- that-be been able to exert such control over what we can and can't do with the culture around us. Our society defends free markets and free speech; why then does it permit such top-down control? To lose our long tradition of free culture, Lawrence Lessig shows us, is to lose our freedom to create, our freedom to build, and, ultimately, our freedom to imagine.

Publisher: Penguin Language: English Date: 2005 Pages: 368

Film:
A Scanner Darkly

Plot: A Scanner Darkly is a 2006 science fiction thriller directed by Richard Linklater based on the novel of the same name by Philip K. Dick. The film tells the story of identity and deception in a near-future dystopia constantly under intrusive high-technology police surveillance in the midst of a drug addiction epidemic.

Starring Keanu Reeves, Robert Downey, Jr., Woody Harrelson, Winona Ryder



Book:
Welcome to the machine:

science, surveillance, and the culture of control

In Welcome to the Machine: Science, Surveillance, and the Culture of Control, Jensen and Draffan take a hart-hitting look at the way technology is used as a machine, to control us and our environment. Most people would be disturbed if you told them that everything from their store purchases to their public transit rides are recorded and filed for government or corporate access. But more often than not, the smooth, silent cleanliness of its operation allows the Machine of Western Civilization to go unnoticed. In this timely and important new collaboration, Jensen and Draffan take on all aspects of Control Culture: everything from the government's policy of total information awareness to a disturbing new technology where soldiers can be given medication to prevent them from feeling fear. They write about pharmaceutical packaging that reports consumer information, which is then used to send targeted drug advertisements directly to your TV.

Chelsea Green Publishing, 15-Sep-2004 - Computers - 285 pages

Where is Hiro Protagonist?

With all the news about SOPA, PIPA, ACTA, Twitter's, Google's and YouTube's new policies and all the other questionable internet regulations doing the rounds of newspapers and media sites, I feel like we need Hiro Protagonist to save us from all this 'digital evil'. I guess it's precisely because of my distress call to Hiro on the Digital Natives Facebook group that this newsletter's editor asked me to speak about this character).

So, who is Hiro Protagonist? Well, he's the heroic protagonist of author Neal Stephenson's dystopian, cyberpunk novel Snow Crash (1995), a dense piece of prose perfection. I fell in love with the book about eight years ago mainly because it projects just the right balance of being a sci-fi action thriller, a detective story and a brilliant satire.

The story's plot is quite straightforward. Hiro is a freelance hacker, music promoter (a trait I identify with as a former music promoter), sword fighter and pizza delivery boy for the mob. He unwittingly gets entangled in the conspiracy of L. Bob Rife, a Murdoch like media mogul trying to rule the world with the help of an ancient neuro-linguistic computer virus; Hiro crushes Rife's operation like a true cyber-samurai with the help of his friends and allies. What makes this story so deeply fascinating to me, however, is the way in which the author paints the picture of a bleak future, as well as the idea that language induced consciousness is actually a virus.

Similar to William Gibson's classic sci-fi novel Neuromancer, the story is located in the real world (USA of course!) and in the Metaverse – Stephenson's 3D version of cyberspace (which became the blueprint for the online simulation game Second Life). In this fictional real world, all important infrastructure and businesses are franchised to such an extent that the country has practically lost its nationhood status. Franchised corporations function as quasi-nations within their own land, with enforceable laws and citizenship. For example, the techno-utopists among you would most likely be citizens of Mr. Lee's Greater Hong Kong. Even the highways and cops are franchised.

Stephenson describes this capital-owned world as environment- and-socially messed up. In order to escape this tristesse (sad reality), you log into the Metaverse via high-tech goggles and a PC that is connected to a broadband fibre optics network. Once in, you interface with 3D representations of the real world and what seems like characters and settings with no "negative" aspects to them; it's a virtually boundless place for possibilities. Yet, there is a digital divide here. For example, poor people have a less coolly rendered avatar and no access to hip places like the VIP club, The Black Sun. Although Hiro is one of the poorer people of this universe, he is a star in Metaverse by virtue of him being one of its first settlers and constituting programmers.

Does the storyline now seem familiar in comparison to our own world and our Metaverse, the Internet? Aren't we already kind of citizens of transnational corporations, in a world driven by a capitalist-orientated globalization? Isn't our life in the virtual space of our PC and social networks to some extent a distraction from the everyday routines we dislike? Our Metaverse is in fact, becoming the normative element of 'dwelling' and our offline routines, the exception.

Even though Stephenson (the author) refuses to subscribe to the label of a "modern day prophet", one cannot but be stunned by how close he comes to mirroring our present lives in his fictional world. Even the idea of the virus ruling our linguistic pathways let's you relook parts of our reality in relation to the fictional world in Snow Crash. So, let me explain the virus, Snow Crash which operates in the real world as well as the virtual.

The effects of Snow Crash are, on the one hand, the alteration of human consciousness in a way that one becomes programmable like a computer, and, on the other hand, it lets every computer system crash, leaving behind the white noise one sees when a TV is set to a dead channel (dancing pixels). With respect to the biological version, one loses the ability to reflect as a human, because the virus puts one in a pre-Babylonian state.

According to the retelling of the Babel myth in this story, the universal human language spoken before the Tower of Babel incident took place, was purely performative. In this pre-Babel society, there were gods who controlled the people and society via Me, a performative script. The Me can be understood as mimicking a recipe for how to bake bread, yet, with the difference that when the Me was perceived, it made the recipient do exactly and immediately what its words said.

One of the Me-controlling gods was Enki, who at some point understood the harm that lies in the viral potential of such a language. Just imagine that the command line "you are sick and you will tell the others you are sick" in the Me language would be equivalent to a real-world creation and spread of the flu virus. Enki therefore wrote a Nam-Shub (a computer worm like Me) that altered the brains of the people and 'crashed their consciousness into reality'; They simply couldn't comprehend each other anymore and therefore had to start reflecting in order to communicate. The villain L. Bob Rife found a way to reverse Enki's Nam-Shub with Snow Crash and infected people behave like zombies, controlled by the media mogul who owns all network infrastructures.

Again, do you see any familiarity with our world? Isn't our consciousness being narrowed, when big media corporations impose on us their perspectives and ideas, and when they try to shut down, with the excuse of piracy, the spaces in which one can reflect and re-contextualise those perspectives and ideas? Haven't the war on terror and piracy become viral concepts that already do or will affect our bodies? Can't we also see in memes or a phenomenon like Anonymous the viral aspect of thoughts? It is those kinds of questions that pop into my head when reading Snow Crash.

But back to the story. Hiro is the hacker that prevents the realisation of L. Bob Rife's vicious plan. How does he do so? Well, by hacking the system and making the people aware of the threat. He re-establishes Enki's Nam-Shub to reverse the biological effects of Snow Crash and writes a code to block the virus in its digital form. He's the hero that prevents the people from falling into the pre-Babylonian state of unconsciousness. And that is why I feel we need people like Hiro Protagonist in order to block us from all those viral threats of today's post-modern society.

By Philip Ketzel

Why Doesn't Washington Understand the Internet?

By Rebecca MacKinnon, New America Foundation

Politics as usual is not compatible with the Internet age, especially when it comes to laws and regulations governing the Web. And the Internet's key players — along with millions of passionate users who have tended to view Washington as disconnected from their lives — are realizing that they can't ignore what happens on Capitol Hill.
In late 2010, on the eve of the Arab Spring uprisings, a Tunisian blogger asked Egyptian activist Alaa Abdel Fattah what democratic nations should do to help cyber¬activists in the Middle East. Abdel Fattah, who had spent time in jail under Hosni Mubarak's regime, argued that if Western democracies wanted to support the region's Internet activists, they should put their own houses in order. He called on the world's democracies to "fight the troubling trends emerging in your own backyards" that "give our own regimes great excuses for their own actions."

The ominous developments that Abdel Fattah warned about are on display in Washington today in the battle over two anti-piracy bills. This fight is just the latest example of how difficult it is for even an established democracy to protect both intellectual property and intellectual freedom on the Internet — all while keeping people safe, too. It is a challenge that Congress has historically failed to meet.

But Washington is waking up to the new reality: Politics as usual is not compatible with the Internet age, especially when it comes to laws and regulations governing the Web. And the Internet's key players — along with millions of passionate users who have tended to view Washington as disconnected from their lives — are realizing that they can't ignore what happens on Capitol Hill. Both sides must now face the long-simmering culture clash between Washington and the Internet, with implications that go far beyond a temporary Wikipedia blackout.
Washington targets isolated, static problems.
On the Web, everything is connected and changing quickly. Politicians started fighting over Internet policy in earnest in the mid-1990s, when the Web emerged as a serious platform for commerce as well as activities from pornography and crime to artistic expression and political activism. The first battles illustrated the perpetual problem with Internet laws: In seeking to protect people, they tend to be shortsighted and overly broad. To most critics, those were the main problems with the Senate anti-piracy bill known as the Protect IP Act (PIPA), which has been delayed pending changes, and the House measure, the Stop Online Piracy Act (SOPA), which has been put on indefinite hold in the wake of a massive public outcry. Similar problems of scope and consequences trace back to the early days of Internet regulation.

Take the bruising political battles over online pornography and indecency. In 1996, Congress passed the Communications Decency Act, making it a crime to "transmit" indecent material to minors over the Internet. In 1997, the Supreme Court declared the law unconstitutional. According to Justice John Paul Stevens, the law threatened to "torch a large segment of the Internet community" because its language was too vague and would infringe on the free speech rights of adults.

In 1998, Congress tried again with the Child Online Protection Act, requiring all operators of commercial Internet services to restrict access by minors if their sites contained "material harmful to minors" as defined by "contemporary community standards." The authors of the bill argued that the same legal logic that works in the physical world should work in the digital world and that protecting minors wouldn't limit adults' free expression.

A decade-long legal battle ensued. The law was never enforced because the Supreme Court found that its definitions and remedies were too broad to avoid stifling protected speech among adults on the Internet.

The cost of getting the law wrong and failing to keep up with technological change is high. In 1986, at the dawn of the e-mail era and several years before the World Wide Web as we know it was invented, Congress passed the Electronic Communications Privacy Act, which allows law enforcement authorities to request the contents of anybody's e-mail without any court order or warrant if the data is stored on the servers of a commercial third-party service for longer than 180 days. Why? Because back in 1986, long before the advent of Gmail, Hotmail and other Web-based services, let alone cloud computing, nobody imagined that people would want or need to store confidential information on remote servers for longer than that.

Thus anything older than 180 days was considered abandoned. In an effort to update the law, Google, Facebook, Microsoft, AT&T and a number of other companies have teamed up with civil liberties groups to lobby Congress. They have been stymied by lawmakers on both sides of the aisle who are concerned about the political consequences of appearing soft on crime.

Lobbyists exert huge influence in Washington.

Major Internet players were late to the game.

The fight this past week is a prime example of lobbying in action. According to the campaign finance research company MapLight, during the 2010 election cycle the 32 congressional sponsors of SOPA received nearly $2 million in campaign contributions from the movie, music and TV entertainment industries, which support the bill, compared with slightly more than $500,000 in donations from the software and Internet industries, which oppose it.

The Internet industry — with its large percentage of start-ups and young businesses — has been slow to lobby, but the big players, led by Google, are scrambling to catch up. Google spent nearly $6 million on lobbying in 2011, according to Opensecrets.org. It threw a lavish holiday party for congressional staffers in December. Facebook has beefed up its Washington office from next to nothing in 2010. And Twitter hired a former congressional staffer to set up the company's office here this past year.

But as Alexis Ohanian of Reddit said this past week: "We spend our money innovating, not lobbying."

That hands-off attitude is partly responsible for SOPA and PIPA. For years, members of Congress have heard from constituents who want them to protect the nation from crime, terrorism and intellectual property violation. They have not faced equally robust demands that online rights and freedoms be preserved. Congress may not get the Internet, but the Internet doesn't get Congress, either.

More than a decade ago, Harvard professor Lawrence Lessig wrote a book about how computer code acts as a kind of law, in that it shapes what people can and cannot do in their digital lives. And, as our digital lives become increasingly intertwined with the physical, it shapes our freedoms as well.
The faith that brilliant and fast-moving feats of engineering and computer code will ultimately triumph over Washington's legal code is one of many reasons most people in Silicon Valley have been inclined to focus on technical solutions to problems, rather than spending their time and money on politics.

Internet companies created the social-media tools that fueled the tea party and Occupy Wall Street insurgencies, and that have helped political candidates rally grass-roots support. Yet before this past week, those companies had not really tapped the power of their own tools to lobby against legislation that runs counter to their interests. Wednesday's Internet "strike" changed that, allowing Web firms to show political muscle in ways that the entertainment industry cannot easily duplicate.
To stay safe in real life, we give up some liberty.

Online, we're not ready to sacrifice freedoms.
In 1996, Grateful Dead lyricist and Internet activist John Perry Barlow wrote "A Declaration of the Independence of Cyberspace." "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace," he wrote. "On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."

In the 16 years since, the government has certainly not left cyberspace alone — because many of "us" have sought its protection from the criminals, pedophiles, bullies, industrial spies, racists, terrorists and others who have invaded the Internet.

Most of us do want the government, which shapes legal code, and the companies, which shape computer code, to defend us against attack and theft: We pay them to do so by giving up a little of our freedom and giving them our taxes, subscription dollars and mouse clicks.

However, the lawmaking norm leans more toward eliminating rather than managing threats online, be they cyber-attacks or intellectual property theft. It has somehow become acceptable to pass laws that presume Internet users are guilty until proven innocent. The Patriot Act and other legislation enable government agents to access a vast range of U.S. citizens' private digital communications without a warrant — or even a suspicion that a specific individual may be involved in a crime, as the law requires for most physical searches.

SOPA also erred on the side of eliminating threats. To protect intellectual property, the law sought to make Web sites liable for their users' activities. This would mean sites would have to monitor all users and block any transmissions or postings that could possibly result in a copyright violation charge.

Washington is driven by geography.

The Internet is global.

Cyberspace, as Justice Stevens pointed out in his 1997 opinion striking down the Communications Decency Act, is a "unique medium … located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet."

Thus a congressman from Iowa can vote "yea" on a bill that ends up affecting Internet users in Bahrain, who have no way of holding him accountable. That is in part because many globally popular online platforms are headquartered in the United States. Moreover, Web services based outside the country that want to be accessible to American users must also comply with U.S. legislation, affecting their users everywhere else.

In addition, governments around the world tend to copy regulations and laws enacted in North America and Europe, particularly when they provide an opportunity to exercise government power through the Internet. In Tunisia, where a new democracy is striving to take root after toppling a dictator one year ago, Islamists and other conservatives point to laws recently passed or proposed in Western democratic countries as evidence that they are in the global mainstream as they seek to reinstate censorship.

For these reasons, activists around the world had good reason to worry that an anti-piracy bill such as SOPA would force overseas Web sites, if they want American audiences, to set up monitoring and censorship mechanisms. Once in place, these would give governments a new set of excuses to demand user information and removal of content.

For neither the first time nor the last time, Washington is trying to wield power over the Internet in a manner that many Americans believe lacks the consent of the governed, let alone the consent of the networked. After Wednesday's protests, the anti-piracy bills are effectively dead or indefinitely delayed. But that doesn't mean the revolution has succeeded.

The computer coding pros — and the millions who depend on their products — have said "no" to legal code they hate. But killing a bad bill is only the first step. The next and more vital step is political innovation. Without a major upgrade, this political system will keep on producing legal code that is Internet-incompatible.
Copyright 2012, The Washington Post http://newamerica.net/publications/articles/2012/why_doesn_t_washington_understand_the_internet_62741

Privacy, Technology and Law

By Barry Friedman

The Supreme Court's decision last week in United States v. Jones presents the disturbing possibility that the answer is yes. In Jones, the court held that long-term GPS surveillance of a suspect's car violated the Fourth Amendment. The justices' 9-to-0 decision to protect constitutional liberty from invasive police use of technology was celebrated across the ideological spectrum.

Perhaps too quickly. Jones, along with other recent decisions, may turn the Fourth Amendment into a ticking time bomb, set to self-destruct — and soon — in the face of rapidly emerging technology.

Dog sniffs. Heat sensors. Helicopter flyovers. Are these "searches" within the meaning of the Fourth Amendment? The court has struggled with these questions over the years.

Writing for the court in Jones, Justice Antonin Scalia looked to the 18th century for guidance. In his view, attaching the GPS was the sort of physical invasion of property the framers had in mind when they wrote the Bill of Rights.

Though Justice Samuel A. Alito Jr. agreed that GPS tracking was a search, he ridiculed Justice Scalia for focusing on "conduct that might have provided grounds in 1791 for a suit for trespass to chattels." For Justice Alito, the risk the GPS posed was loss of privacy, not property. Instead the question was whether long-term GPS tracking violated today's "reasonable expectations of privacy," not those of another era. As a matter of existing doctrine, he asked the right question, but when applied to the government, the standard he used could turn our lives into the proverbial open book, and soon.

Focusing on public expectations of privacy means that our rights change when technology does. As Justice Alito blithely said: "New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile."

Via: http://www.nytimes.com/2012/01/29/opinion/sunday/in-the-gps-case-issues-of-privacy-and-technology.html

A case against online privacy

Summary: Privacy on the Internet is a flaring debate. Given how Facebook keeps flirting with user data and ISPs tracking users' Internet surfing, there is no privacy on the Internet.

By Naman Kakkar

The world went crazy with privacy concerns last month over news about Facebook tracking users even after they logged out was made. (It has to do with cookies.) Oh how the private lives were being spied on by Mark Zuckerberg caved in a bunker with the rest of the Facebook employees monitoring and tracking every Facebook user much like Lucius Fox and Batman; only to sell this data to scamming advertisers and pesky telemarketers who want to sell every married guy a pair of lingerie for he searched about what women like or the telemarketer from Bangladesh who will keep calling you to buy a plastic squeeze to fart cow since you played Farmville. Oh how dare you Zuckerberg?!

Then Jeff Bezos unveiled Amazon Silk — the browser that will predict your next click based on what other users clicked. I knew that Bezos had evil plans with that Amazon Kindle. He even looks like Lex Luthor, I knew it! He was up to no good. Privacy Jeff! Privacy! I don't want you to know that I will click on the nude Lindsay Lohan link after reading about her recent kerfuffle on TMZ's website. RESPECT MY PRIVACY AMAZON!

Of course all this privacy noise comes with no explanation as to what's wrong if Amazon tries to study what their users are doing on the Internet. Here's what happens if Facebook, Amazon, Bing, Google study user behavior:

- Tailored search results
- Better browsing experience

The computer finally does what it's supposed to—start helping you in everyday life. Then there is the advertiser argument. If I read about men's fashion on Facebook, the ads lead me some great websites like PRIVE or Gilt. They show me stuff that I might buy instead of emoticons to download. I've found and bought stuff through Facebook's tailored ads. Another argument is Facebook making money through my data. "O. M. G. Zucky, u r rUDe!"

So essentially, these guys want Facebook to keep offering uninterrupted cloud storage and a medium to communicate for free and not make any money to maintain/run the service. Fair enough, dumb people exist. Let's put this in perspective: Facebook collects user data to study user behavior then shares this data with advertisers who then show you with results that might be relevant and useful to you. For argument's sake this unethical and Facebook says we'll start charging users monthly subscription fees. This model will fail since there is an entry barrier and less users will be willing to use the service. This destroys the whole social aspect of Facebook since less of my friends and their friends will be on Facebook—everybody loses.

I understand privacy concerns but what I can't rationalize is what is wrong with Facebook or Amazon tracking me. They're doing so to:

- make money
- (as a side effect) provide me some value

Compared to ISPs who know everything I do, store this data for 7 years and willing share this data with cops or cap my Internet speeds if I download too much? Let's see:

- service that knows what I do and provides me a better experience
- service that won't tell me I'm being tracked, share this data with the cops and provide me NO benefit

...I wonder who's more dangerous. From all the social media privacy rhetoric, it's clear that an opt-in service or an opt-out option makes people more comfortable about sharing information which isn't private in the first place. But the power suggestion and perception is strong. Also, please cut the crap with all the privacy BS since clearly there is no downside unless citizens of India, Iran, North Korea, Pakistan keep feeding American servers through networks like Facebook/Twitter only so that this data can be used by the CIA to study the country and fly unmanned drones to attack.

Taking cue from The Matrix, I'll put this way: If you're on the Internet... there is no privacy.

Via: http://www.zdnet.com/blog/btl/a-case-against-online-privacy/59662