
DIGITAL
FREEDOM

Almost 50 years have passed since ARPANET, the military network many consider the birthplace of what we came to call the Internet. But the time period saw more than just developments in digital communication. Protests and social conflicts shaped the era, and underscored the emergence of many civil rights movements. Hippie culture also began to gain mainstream attention and influence.

The spiritual successors of these movements are still here – and are prominent influences on digital culture. Remix culture, creative commons, free education, liking, sharing – they're all quite prominent on the Internet.

HIPPIE CULTURE CELEBRATED SHARING, BUT THEY ALSO EMPHASIZED THE IMPORTANCE OF INDIVIDUALITY.

This is the point where the providence of the past diverges from our reality. Some things were never meant to be shared. They were meant to remain private.

PRIVACY IS A HUMAN RIGHT. PRIVACY MAKES US HUMAN. INDIVIDUALS.

WHO ARE WE?

Hello there. We're a Finnish company called F-Secure, and for the last twenty-seven years we've been making software that protects people's data. Wherever people go with their computers, laptops or mobile phones, we've made it our business to create great software to protect the irreplaceable.

Last year, at re:publica 14 in Berlin, we proclaimed the right to Digital Freedom with Freedom Ambassador David Hasselhoff. We called for your contributions to formulate a manifesto for Digital Freedom, a way of raising global awareness about the issues we are facing. The following pages are the crowdsourced and condensed result of your and our efforts, the Digital Freedom Manifesto.

EVERY BODY IS US.

People all around the world added their voices to contribute to this manifesto. The human rights of people from all over the world are deteriorating online, making this an issue that touches everyone.

This document alone is not going to change the world, but Digital Freedom is worth fighting for. We want to contribute to this fight and make it easy for everyone else to know what we are fighting for and why.

TOGETHER. WITH YOU.

The Internet is more than a bubble of us, sitting here, being aware. In order to make this a mass movement, we as people have to understand that the Internet has become the world's nervous system, connecting everyone with anyone at any time.

WE,

AS PEOPLE,

have to understand that even though surveillance is on its way to becoming pop culture, it's not a mere joke on network television or your favorite web series.

WE,
AS PEOPLE,

have to understand that our identity is emergent, is more than the mere sum of its entities. The Internet permeates everything that surrounds us, so every action and every memory that makes up our identity, is mediated through a digital network. We lose control over our own self.

WE,
AS PEOPLE,

have to understand that while this might not bring harm to most people out there right now, we cannot predict the future. What will our data and identities become in the hands of the governments, corporations, and criminal organizations of tomorrow?

However, if there is one thing we want
to convey with this manifesto, it is this:

HOPE.

It was the one thing that echoed through
all of the contributions.

HOPE FUELS ACTION.
HOPE IS THE MOST TENACIOUS PIECE OF EQUIPMENT WE HAVE.
HOPE IS KNOWING THAT CHANCES WILL BE THERE FOR THE TAKING.

HERE'S WHAT WE CENTER OUR HOPES ON.

MANIFESTO THEMES

THE STRUCTURE OF THE MANIFESTO

We've split the manifesto into four clear chapters:

❶ MASS SURVEILLANCE ❷ DIGITAL PERSECUTION ❸ DIGITAL COLONIZATION ❹ RIGHT OF ACCESS, MOVEMENT & EXPRESSION

WHOLESALE SECRET SURVEILLANCE

What could be more important to our organization than the battle for Digital Freedom?
Who could imagine that at the end of 2014 we would need to protect people against governments as well as cyber criminals?

CORPORATE BIG BROTHER

In a world in which everything online is seemingly free of charge, are we willing to accept that corporations such as Google, Yahoo!, Twitter or Facebook can do whatever they like with our personal data?

DIGITAL SOCIETY & CULTURE

We are slowly coming to realize that Angela Merkel was right that, in terms of law, government, crime prevention and international affairs, we find ourselves in Neuland. Digital society is still in its infancy and we intend to be part of shaping it.

DIGITAL PERSONALITIES

Cyber-mobbing, racism, sexism, homophobia and bigotry- one person's freedom of speech is another's repression. How do we approach such behaviour in a community that is fundamentally anonymous?

1

MASS SURVEIL LANCE

“We should be free to vote without anyone else knowing, without intimidation, without punishment. Otherwise, there can be no democracy. We should be free to be who we are, to think our own thoughts, to discuss our own ideas in private, as well as in public, without fear, without persecution.”

MASS SURVEILLANCE BY SECURITY SERVICES WORKING IN SECRET, WITHOUT SUPERVISION OR OVERSIGHT, THREATENS THESE FREEDOMS.

Even George Orwell couldn't have imagined how the greatest innovations of our time – the Internet and smart phones – could be used as tools of government surveillance.

The problem with tools of mass surveillance is that they don't just spy on crime suspects. They're also about spying on people that governments know are innocent.

BULK DATA COLLECTION BY AUTHORITIES IS A GROSS VIOLATION OF THE UNITED NATIONS' UNIVERSAL DECLARATION OF HUMAN RIGHTS, ARTICLE 12.

“NO ONE SHALL BE SUBJECTED TO ARBITRARY INTERFERENCE WITH HIS PRIVACY, FAMILY, HOME OR CORRESPONDENCE, OR TO ATTACKS AGAINST HIS HONOUR AND REPUTATION. EVERYONE HAS THE RIGHT TO THE PROTECTION OF THE LAW AGAINST SUCH INTERFERENCE OR ATTACKS.”

THE LAST DAY OF MASS DIGITAL SURVEILLANCE

By Mike Harris, Director of 89up,
and Campaign Director of Don't Spy On Us
@mjrharris

On October 7, 1989, Soviet tanks ran through the streets of East Berlin in front of the leader of the German Democratic Republic, Erich Honecker to celebrate the Communist regime. Six months previously, Tim Berners-Lee, a scientist at CERN wrote a proposal to his boss for a new information management system. In small, cautious hand-writing at the top his boss had remarked, "Vague, but exciting". This proposal would become the World Wide Web.

Just as Honecker could not foresee the collapse of Berlin Wall, nor could anyone predict how essential the World Wide Web would become to our everyday lives. These are two moments of freedom, just six months apart that have shaped the modern world. A third such momentous day - the last day of mass digital surveillance will one day be upon us.

It won't happen by accident. As citizens, we need to make mass population surveillance as unacceptable as the use of landmines, or the use of CFCs. The harm that mass population surveillance does to the fabric of our society must be debated and we will need to persuade our political leaders that, in amongst all their other priorities, that surveillance reform is essential. This won't be easy. The harm is mostly invisible, like passive smoking, or the hole in the Ozone layer. Yet, with concerted action we can, like in these two examples, make a difference. Here is how we can end digital surveillance.

EDWARD SNOWDEN

We would not be having this debate if it were not for an American security contractor, Edward Snowden. Snowden blew the whistle on programmes that had expanded the scope of surveillance beyond anything imaginable by politicians or even the public.

The US Congress and Senate were not told that tens of millions of citizens had been placed under surveillance by the NSA. GCHQ in the UK had not informed Parliament that it was actively capturing all the data from undersea cables off the coast of Cornwall. The NSA was monitoring the phone calls of German Chancellor Angela Merkel. All these programmes were shrouded in secrecy and not subject to normal democratic oversight. Politicians suspended their critical faculties when it came to the work of the intelligence agencies. The agencies were put beyond scrutiny - and as a result the scale of their ambition grew unchecked until they began to tell each other they could "master the internet".

Snowden acted alone, and took sole responsibility for his actions. In Laura Poitras' film, CITIZENFOUR, she captures the moment Snowden decides to go public and reveal himself as the NSA whistleblower. Snowden's actions were motivated by an early recall of the potential the internet had. He remembered the days when students would debate with nuclear physicists online, when people were using the Internet for experiments to create new currencies, new ways of communicating and radical ways of doing business. **"I remember what the internet was like before it was being watched, and there's never been anything in the history of man that's like it."**- Edward Snowden in CITIZENFOUR

Surveillance chills this openness; it makes us restrict our free speech. A 2013 survey of writers by PEN American Center found that 73% of respondents said they have "never been as worried about privacy rights and freedom of the press as they are today" with nearly 1 in 6 avoiding writing or speaking on a particular topic due to their fears over surveillance. A further PEN survey in 2014 found 61% of writers in "not free" countries self-censored due to the risk of surveillance. This is perhaps unsurprising. What is perhaps more concerning is that even in countries considered free, a significant 34% of writers were self-censoring due to surveillance. We have to reclaim our right to free expression and privacy.

HOW CAMPAIGNS CAN CHANGE THE WORLD

Campaigns can change the world. There is no inevitability to the status quo. Landmines were once just another weapon in humanity's wide arsenal of ways to murder. They maimed over a million people and were killing 26,000 people a year before the landmine ban came into force. Now that figure is 4,000 people per year and falling. This is thanks to a coalition of over 100 NGOs who came together in 1991 to try and secure a global prohibition on the use of landmines. In

the face of opposition from 3 of the 5 UN Security Council permanent members (China, Russia and the USA), 80 countries still worked together and committed to a global prohibition.

At a global level much has happened since the Snowden revelations that should give us hope that our campaigning can change the world. In just over a year and a half, 416 international civil society organisations have backed the 13 "Necessary and Proportionate Principles" that aim to provide a benchmark to help states reform. On 18 December 2013, the UN General Assembly passed 'The right to privacy in the digital age' opening up an avenue for the 13 principles to be considered as components of the fundamental right to privacy. This gives global civil society a real opening.

Yet, we also need individual countries to take action. It's hard to see authoritarian China deciding to set an example and disbanding their army of 250,000 "50 cent party members" who monitor online content in real time. So we need democracies to set an example. In a survey of civil society, nearly 1 in 3 participants said a major debate had been started in their countries on surveillance. In Austria, Brazil and Canada the debate has been particularly vibrant. But there are two countries, the US and the UK, who have the most intrusive surveillance programmes of any democratic states. In these two countries, debate is not enough.

This is why 6 of the leading privacy and freedom of expression organisations have come together to fight back against surveillance in the UK. ARTICLE19, Big Brother Watch, English PEN, Liberty, Open Rights Group and Privacy International (the 6 core members) are joined by affiliates including Amnesty International, Amnesty UK, AccessNow, Centre for Investigative Journalism, Electronic Frontier Foundation, IFEX, Index on Censorship, Public Concern at Work and Open Democracy. This is an unprecedented coalition has a single aim: the get reform of the law in the UK to end mass population surveillance. The challenge is real – not one of the UK's 3 main political parties condemned the scale of GCHQ's surveillance in the aftermath of the Snowden revelations. As Snowden himself pointed out, GCHQ has developed the world's first "full take" of the Internet capturing the entirety of the data entering the UK in one significant location.

Our campaign has distilled the 13 international principles into 6 principles to get the law right in the UK.

Our principles are:

1 NO SURVEILLANCE WITHOUT SUSPICION

Mass surveillance must end. Surveillance is only legitimate when it is targeted, authorised by a warrant, and is necessary and proportionate.

2 TRANSPARENT LAWS, NOT SECRET LAWS

The Government is using secret agreements and abusing archaic laws. We need a clear legal framework governing surveillance to protect our rights.

3 JUDICIAL NOT POLITICAL AUTHORISATION

Ministers should not have the power to authorise surveillance. All surveillance should be sanctioned by an independent judge on a case-by-case basis.

4 EFFECTIVE DEMOCRATIC OVERSIGHT

Parliament has failed to hold the intelligence agencies to account. Parliamentary oversight must be independent of the executive, properly resourced, and able to command public confidence through regular reporting and public sessions.

5 THE RIGHT TO REDRESS

Innocent people have had their rights violated. Everyone should have the right to challenge surveillance in an open court.

6 A SECURE INTERNET FOR ALL

Weakening the general security and privacy of communications systems erodes protections for everyone, and undermines trust in digital services. Secret operations by government agencies should be targeted, and not attack widely used technologies, protocols and standards.

So far, 10,000 people from across the UK have signed up to our campaign and our 6 principles - thousands have attended live events on surveillance - we hope still more will make their voices heard during the general election campaign.

With the general election on the horizon, as citizens we've got huge leverage to secure commitments from parliamentary candidates to protect our privacy and free speech. Without political support for reform, the change we need is simply inconceivable.

1 MASS SURVEILLANCE

Thanks to our partnership with F-Secure, this change is more possible. F-Secure's support for the Don't Spy On Us day of action, where 500 people stood up for our human rights in the heart of Shoreditch, the UK's biggest tech hub, drove awareness of this issue. We hope more companies also take a stand for our rights and work with civil society to fight back.

NOW, OR NEVER

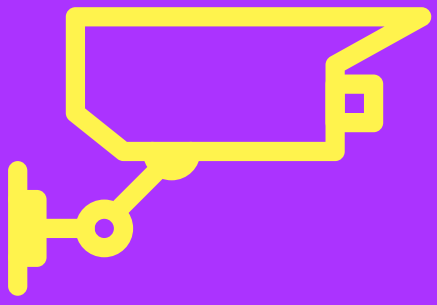
No one could have predicted that a US security contractor would blow the whistle on surveillance. In response, hundreds of thousands of people globally have joined campaigns. The European Parliament, the Council of Europe, the United Nations and national parliaments have all condemned mass population surveillance too. The momentum isn't slowing. But, like Snowden's actions and the fall of the Berlin Wall, the outcome isn't pre-determined. No one predicted the Berlin Wall would be built either.

For campaigners - it's now, or never. We need to persuade our political leaders that "mastering the Internet" is not an acceptable aim. Our freedom to think, write, converse openly - or in private - is a freedom worth preserving. It's time for governments to support action at the UN to adopt the 13 principles as global principles. In the UK, we need new legislation to roll back surveillance.

WE CAN MAKE THE LAST DAY OF SURVEILLANCE HAPPEN.

2

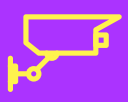
DIGITAL PERSECUTION



“THE INTERNET IS NOT AN EXTRALEGAL SPACE”

– a phrase popular in discussions about file sharing and entertainment piracy.

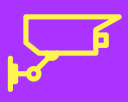
PEOPLE SHOULD BE PRESUMED INNOCENT UNTIL PROVEN GUILTY, IN BOTH NATURAL AND VIRTUAL SPACES.



A PERSON'S DIGITAL POSSESSIONS SHOULD BE GRANTED THE SAME PROTECTION AND RESPECT AS PHYSICAL BELONGINGS, EVEN IF A STATE CONSIDERS YOU A "FOREIGNER".

The ability to collect and store private data in perpetuity must be stopped.

All courts that approve surveillance activities should be forced to reveal their decisions to the public.

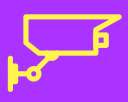


AUTHORITIES INVESTIGATING CRIMES AND OTHER REAL SECURITY THREATS SHALL TARGET NAMED SUSPECTS WHEN COLLECTING DATA.

Every such action should be based on a warrant by a legal and transparently acting court of law, and supported by a substantiated suspicion.

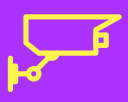
REQUESTS FOR DATA SEARCHES BY LEGITIMATE LAW ENFORCEMENT AUTHORITIES SHOULD NOT BE BASED ON CONCEPTS DERIVED FROM OUTDATED TECHNOLOGY.

They should not presume the application of one country's code of law and conduct onto another country, but on a mutual framework that observes common human and property rights.



THE CONTRIBUTORS EXPECT THE FOLLOWING ACTIONS:

- Enforce an international standard that binds Internet companies and governments to certain transparency standards in data collection and usage policies.
- Acknowledge digital data as physical property, worthy of protection and discretion.
- No data collection by law enforcement without suspicion and warrants.
- No prioritization of comfort over the principles of data avoidance and data minimization.



By Ewen MacAskill

The Snowden revelations have had reverberations all around the world. Snowden sparked a debate on the balance between security and privacy. He created a consumer backlash still being felt by the mega-internet providers such as Google and Microsoft. He has caused international rifts: between the US and Russia, Brazil and Germany; and between Australia and Indonesia.

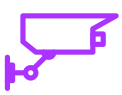
On top of all this, there has been the personal drama of Snowden himself, America's most wanted man, fleeing Hong Kong to end up in exile in Russia. The story has so far spawned two books, a fly-on-the wall documentary, two proposed movies - one by Oliver Stone and the other by Barbara Broccoli - and a graphic book.

There has been one major exception to all this: Britain. Its surveillance agency GCHQ (Government Communications Headquarters) has been at the centre of the row, along with its close partner America's NSA. Snowden said GCHQ is worse than the NSA. The Guardian, which was the first to publish the revelations, is London-based.

In spite of this strong British presence in the story, the debate has been subdued. The public appears to be apathetic, compared with countries elsewhere in Europe, particularly Germany. There has been little discussion in parliament. Other than the Guardian, most of the media, including the BBC, has largely ignored it.

Why this muted response in the UK compared with the US, much of the rest of Europe and elsewhere in the world? No-one seems to have a definitive answer. I have spoken at various venues throughout the UK over the last year: to groups of journalists, to lawyers, to academics, post-film discussions and fringe meetings at the Labour and Liberal Democrat conferences. It is rare that someone will not raise the issue of why Britain appears to be so indifferent and what can be done to motivate people.

I can understand some of the hesitancy on the part of the British public. I was one of three journalists who interviewed Edward Snowden in Hong Kong a year and a half ago. Although I knew it was a big story, I seriously underestimated just how big it would become.



The night before publication in the Guardian of the first of the stories, the Verizon one indicating the scale of the NSA's bulk data collection, I was discussing it with then Guardian colleague Glenn Greenwald, in his room at the W hotel in Hong Kong. I wondered if the story was too narrow, too technical.

A few hours later we had our answer, with US television, papers and social media in a frenzy to follow up the story. The next story was even bigger, PRISM, about the relationship between the NSA and internet providers. After that, the controversy just kept growing, culminating a few days later in Snowden outing himself as the source. Further stories were published in the following months - in the Guardian, Washington Post, the South China Morning Post, New York Times, Der Spiegel and O Globo - and have continued through to today.

The most charitable explanation for why the response in the UK has been so muted would be say that the British public found the documents - sharing the same doubts as I had about the initial Verizon document - too technical. As an explanation, it does not work. If readers and viewers elsewhere round the world were not put off by the technical aspects of the documents, why should Britons?

A better explanation is historical. Britain has enjoyed relative stability for close to four centuries, with the last major upheaval the English Civil War (or if you want to be picky the 1688 Glorious Revolution or the 1745 Jacobite Rising). Contrast that with say Germany, where the Snowden revelations have had a special resonance because of the Stasi, with its systematic collation of the personal details of citizen after citizen.

A further explanation is that there is a different attitude in the UK towards the intelligence services, who are generally viewed positively. It is not just cultural, with the prevailing view of spies shaped by the James Bond movies.

The image of the intelligence agencies is overwhelmingly positive in Britain. In spite of the abuse of intelligence to justify British involvement in the run-up to the 2003 war in Iraq and other controversies, there is appreciation for the part they have played in countering the IRA bombing campaign and helping behind-the-scenes to negotiate a ceasefire, and more recently in combating Islamist terrorist plots.

Another explanation for the apparent apathy, a peculiarly media one, is the antipathy felt towards The Guardian from its British media rivals. That antipathy has increased over the last few years as a result of The Guardian investigations into phone-hacking and other abuses that have seen journalists on other papers jailed and Rupert Murdoch's News of the World closed.

The collective response of the British media was to either ignore the Snowden revelations or to attack The Guardian for publishing what was viewed as state secrets that might endanger operations or even lives.

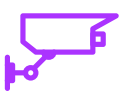
The Daily Mail, in October 2013, smeared The Guardian, describing it as the "the paper that helps Britain's enemies". At least one Mail columnist called for Guardian journalists to be jailed.

Attacks from the Mail are unsurprising. What was disappointing though was the attitude of the BBC, which rarely treated the Snowden stories as major news. The BBC retains huge power in the UK and its lack of interest in pursuing the story is one reason why the Snowden revelations have failed to enter British consciousness.

Overall, the British government has taken a harder line towards The Guardian compared to the authorities in the US. The organisation has been threatened with legal action to prevent it publishing the documents. The computers on which the documents were stored and written had to be destroyed under the supervision of two GCHQ officials in the basement of Guardian headquarters in London, a purely symbolic act given the documents remained intact and available to reporters in New York. And Greenwald's partner, David Miranda, was held for nine hours at Heathrow Airport under terrorism legislation.

The political alignment in the UK has not helped. Normally the Liberal Democrats, the party most concerned about civil liberties issues, could be relied upon to run with issues such as surveillance. Some of its MPs, such as Julian Huppert, have done so and the party leader Nick Clegg has made one sympathetic speech, though leaving the issue until after the election. But the Liberal Democrats are in coalition with the Conservatives - Clegg is deputy prime minister - so are not pressing on the issue.

The Labour party is not pushing it either, not seeing it as an issue that much interests the electorate.



❷ DIGITAL PERSECUTION

It is not all bad news. It may yet turn out that Britain is just a slow burn. There is a gradual acceptance among some politicians, civil servants and intelligence officers - as well as in the private sector and among journalists and academics - that there is a debate to be had about the balance between security and privacy.

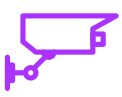
Changes may be forced on the British Government by courts in Europe or by the internet provides such as Google providing encryption as a normal part of its service.

There is a grudging acceptance among some in the inner circles of government and the intelligence agencies that the initial responses to the Snowden were not well-handled, both in the failure to engage in dialogue with The Guardian over the revelations and in the heavy-handed over-reaction (though there are some in the intelligence agencies still arguing that the government should have taken a much harsher line, cracking down on The Guardian at the outset).

While public support for GCHQ and the other intelligence services remains high, there is recognition within the intelligence agencies that they have a public relations job to do. The new head of GCHQ, Robert Hannigan, within weeks of taking office, opted against maintaining the traditional low profile and wrote an article for the Financial Times warning about the difficulties being created for the surveillance agency by internet providers through the widespread introduction of encryption.

The article is a testimony to the impact of Snowden: GCHQ prepared to go public. Hannigan's article is also recognition that encryption being introduced by the private sector must work to some extent if it is causing the agency concern.
There is some pressure to reform after the election legislation governing surveillance, the Regulation of Investigatory Powers Act (RIPA), which is near incomprehensible in parts, perhaps deliberately. The response of the government in the first few months after Snowden was that it is all working well and did not need reform, even though RIPA was written in 2000, before the spread of social media. That line has not held.

The new line is that the government is willing to rewrite parts of it to make it more comprehensible but not making any real concessions. That line is unlikely to hold either.



Privacy almost certainly will not be an issue in the British general election in May. But a debate of sorts is at least underway.

The debate could go either way. If there was to be a major terrorist attack in Britain, it would be even harder for privacy activists to persuade the public there needs to be less surveillance.

Alternately, one of the two proposed Snowden movies might help raise awareness in Britain about the scale of intrusion and loss of privacy.

IT IS A SLOW BURN. BUT THE FLAME MIGHT YET CATCH.

3

DIGITAL COLONIZATION

If the United States is unwilling to conform to the privacy rights written into its own founding charter or expand them to foreigners, governments outside of the US must invest to create competing Internet service clusters around the globe.

HUMAN RIGHTS DON'T STOP AT NATIONAL BORDERS.

IF ALTERNATIVES RISE, SOFTWARE COMPANIES IN THE USA WOULD BE FORCED TO ADOPT PRIVACY CONCERNS TO DEFEND THEIR MARKET SHARE.

TO ENCOURAGE REAL COMPETITION, GOVERNMENTS AROUND THE WORLD (INCLUDING THE EUROPEAN UNION) MUST CONTINUALLY RENEW THEIR RESPECT FOR SECURITY, PRIVACY AND HUMAN RIGHTS. INNOVATIONS AND START-UPS ALONE CANNOT CHANGE LAWS.

THE CONTRIBUTORS EXPECT THE FOLLOWING ACTIONS:

- Bind globally acting companies to adhere to the laws of the individual countries they do business in.
- Establish the infrastructure, bureaucracy, and educational and legal frameworks needed to foster local Internet companies, and grow them to challenge the quasi-monopoly of US-based Internet services.

FUCK OPTIMISM

by Cory Doctorow,
doctorow@craphound.com

I'm an activist and a science fiction writer, so it's only natural that people ask me whether I'm optimistic or pessimistic about the future.

But optimism and pessimism are both a form of prediction. Whether you're bullish on the future that's coming, or terrified of it, you're effectively saying that the future *is* coming -- it's a thing that *happens to us*, not a thing that *we make*. If I believed that the future was foreordained, that it would come or not come regardless of what I did, I don't know why I'd bother getting out of bed (except, perhaps, that in the foreordained future, I am predestined to get out of bed).

Prediction is a foolish pastime, and science fiction writers, better than anyone, should know this. Almost none of science fiction's predictions since Mary Shelley have come true, and when people laud science fiction's capacity to predict, they tend to cherry-pick those few predictions that did come true (and really with all those predictions from Shelley to now, the remarkable thing would be if *none* had come true), they're like the man who fires a shotgun into the side of a barn, draws a bullseye around the target, and expounds on his excellent marksmanship.

Science fiction writers who believe in their own predictions are like drug dealers who sample their own product. It never ends well.

Let's talk about pessimism for a moment. Say that I believed that the chances are that the Internet -- the nervous system of the twenty first century, which has the power to allow any two people to speak to one another without being interfered with by a third, which has the power to allow us to communicate in privacy and secrecy so perfect that the only way to violate it is to physically coerce one of the communicants into revealing the discussion, because the messages themselves

are impervious to technical eavesdropping -- that this Internet that I loved and built and wrote and labored for would be perverted by the forces of reaction, greed, fear and authoritarianism.

Say that I believed that the Internet -- presently treated by regulators as the world's best video-on-demand service, or the world's most perfect pornography distribution service, or the world's finest jihadi recruiting tool -- would be turned into the world's greatest surveillance device.

WHAT WOULD I DO?

I would work to take back the Internet. To make crypto usable and robust. To spread free (as in "speech", if not as in "beer") and open software. To hold regulators to account on the matter of network neutrality, and to build alternative networks less susceptible to rent-seeking by venal cultists of the religion of fiscal responsibility over human decency.

In short, I would do every single thing I would do if I was *optimistic* about the Internet.

FUCK OPTIMISM.
I WANT *HOPE*.

Hope is why you tread water if your ship sinks in the open sea: Not because you have any real chance of being picked up, but because everyone who was picked up kicked until the rescue came. Kicking is a necessary (but insufficient) precondition for survival.

There's a special kind of hope: the desperate hope we have for people who are depending upon us. If your ship sinks in open water and your child can't kick for herself, you'll wrap her arms around your neck and kick twice as hard for both of you.

To quote the eminent sage and Saturday morning cartoon superhero The Tick:
"Don't destroy the Earth! That's where I keep all my stuff!"

The Internet is the nervous system of the twenty-first century and it connects everything and everyone I love on Earth, and so I want hope to give me the energy to kick for all of it.

We have given rise to a race of post-human, immortal, uncaring superbeings, called transnational corporations. We humans are their gut-flora, tolerated so long as we help them get on with their metabolic processes, but treated as pathogens when we threaten their well-being.

Historically, rulers have plumped for wealth redistribution to create social stability -- because social services, mercy and kindness were cheaper than the guard-labor and surveillance necessary to get the same quantum of stability. Technology has automated surveillance and retribution to a terrifying degree, and we are now living its consequences: a monied elite that has taken off the gloves and uses surveillance and militarized policing in place of social justice and basic fairness.

It's hard to be optimistic in the Thomas Piketty Singularity. It's easy to be pessimistic when our entertainment technology becomes a means to both total surveillance and automated, algorithmically assigned guilt -- we have discovered that we don't have to choose between Orwell and Kafka, we can have both! And what's more, we can get there by way of Huxley!

But Huxley, Orwell and Kafka didn't take away hope, they gave it to us. They gave us the words to describe the present (not the future, though the present is the moment at which the past becomes the future, so they're related). They gave us the cognitive tools to conduct the argument about the society we want to build, the how we want out technology to serve us.

THEY TAUGHT US HOW TO KICK. NOW IT'S UP TO US TO KEEP HOPE ALIVE, AND KICK UNTIL WE RESCUE OURSELVES.

4

RIGHT OF ACCESS, MOVEMENT AND EXPRESSION

"IF YOU HAVE NOTHING TO HIDE, YOU HAVE NOTHING TO FEAR."

This statement is only true if you assume that the people watching you have only your best interests in mind – that they are fair and honest, and will never abuse their power.

HOW CAN WE BE SURE NOW? HOW CAN WE KNOW THIS WILL BE THE CASE IN THE FUTURE?

WE CAN'T.

THE MORE SECRETIVE GOVERNMENTS ARE, THE LESS SURE WE CAN BE. AND THE LESS WE SHOULD TRUST THEM.

GOVERNMENTS CHANGE, AND SO DOES THEIR STANCE ON FREEDOM.

That is why we should make sure we limit the power governments, police, and security services have over our Digital Freedom.

What we say and write in private should be of no interest to any government or government organization. We should fight for freedom of access to platforms, freedom of movement, and freedom of expression.

THE CONTRIBUTORS EXPECT THE FOLLOWING ACTIONS:

- Limit the power of governments, police and security services in digital spaces.
- Facilitate everyone's access to communication platforms without bias.

THE EXTENDED MIND

By Peter Warren

Ten years ago, a 30 metre high wall of water caused by an undersea earthquake hit the coastal communities of South East Asia killing 230,000 people, its long-term impact was even greater, it dislocated communities, split families and as well as wiping out life, it also wiped lives clean.

Typical among its victims were Mustafa, an Indonesian businessman and his 14 year old daughter Rina. Mustafa lost his wife and daughter (Rina's elder sister) and the house that they lived in was virtually destroyed. Along with their family, their memories and the bric-a-brac that made up their lives and their former identity was washed away.

Mustafa and Rina were not alone when they said that, 'they had lost everything.'

Such experiences, while not on the same dramatic scale, are not uncommon. They happen to nearly all of us because of a common misconception about identity and what goes into creating it.

It is a little known philosophical concept known as 'the extended mind,' that the technology industry and governments are now acutely focussed on, because for most of us our memories are in our surroundings and in our mementoes: and now more and more; those memories, thoughts, desires and dreams are making their way onto our laptops, tablets and mobile phones.

Put simply, the extended mind is the web of memories, places, objects, actions and things that go to make us up.

"It's the idea that our minds are not confined to what goes on inside our skulls, but that other information processes like our notebooks, our environments, maybe other people, or our laptops, also contain some parts of our minds, or parts of our memories," said Oxford University's Professor Nick Bostrom, the Swedish head of the Faculty of Philosophy and Oxford Martin School, who is also Director of the Programme on the Impacts of Future Technology.

Our smartphones have become a lumber-room of our extended minds and have the power to yield huge amounts of information, a store that technology companies like Google and Facebook are eager to exploit. Google already offers identity verification services to several US Government departments and it is using our data to profile us, acquiring more information on us improves the service they offer.

All of us have special memories and places – a waterfall, a theatre, a park bench – places that had some significance in our past and are part of our extended mind. We store our souvenirs, our artefacts, in attics and garages in the belief that we can access and refresh a memory when the need arises.

Now we are being encouraged to preserve that memory by putting it into a digital vault, our memories are stored in our photos and our GPS data, but in return for the technological tools to be able to do this, companies and governments now demand unfettered access to our information, as Edward Snowden has revealed.

Poets and philosophers have reflected on the fact that we all have a different memory of events. Now, all that has changed because the technology companies want to make money out of the data of our extended minds. The companies are ensuring that not only can we never forget, but also that we are never allowed to forget.

And the reason is simple. Our identity and our memories are being sold to nearly every company in the world so that they can identify the particular individuals who fit a profile. The companies profile those individuals from the data culled from their extended minds: the things that they like, their opinions and the places that mean most to them.

This big data world allows technology companies to even work out who our friends are. For example, if they search for clusters of credit cards numbers and note the time and place where they are used, companies can find out who knows who. Ironically, this pursuit of our basic data is robbing us of our misconceptions of the past, ironing out and homogenising differences and, for the first time, generating a shared memory grounded in hard data.

Social media is now a shared mind, a collective memory.

Writers have warned us about this type of mind control, from Dickens's Thomas Gradgrind in Hard Times to the bleak authoritarian surveillance regime of George Orwell in 1984. It is a world of facts where human frailty (the thing that makes us human) is being progressively lost – while we ourselves are unable to be get lost, because of our satnavs and unable to forget, because of the mass of data stored on us by our friends in social media and the companies that harvest those memories.

We also lose a central theme of our existence, being lost is an idea that has been a stock in trade of books and films since the beginning of the written word. Taken to its logical extreme, we will never ever be lost again, not even to death.

Dr Jonathan Cave of Cambridge University's Centre for Science and Policy says we lose this human frailty at our peril.
"One of the things that computer scientists believe is that if we can be freed from some of the weaknesses that we have, that we become effectively immortal because death no longer becomes a problem, because we can preserve the mind and refresh the body and the weaknesses of memory or dementia can be made to recede."

So our past and the events that make us could be stored on a USB stick and then inputted into a clone of ourselves. For many, an attractive prospect, however, it also means that all our data, all of our identity could also just as easily be stolen.

Indeed, you could argue that, in some senses, a copy of our data could be built into an entity that knows us better than we know ourselves, since modern databases now have some 1,500 data points about every individual's life.

Yet this more 'complete' view of our identity – whilst technically our data record – is not how we perceive ourselves, and so is not our identity at all.

We are losing fundamental human rights, the right to be forgotten, the right to lose our way and the right to be forgiven – all key parts of our life and our culture until now.
Viktor Mayer-Schoenberger, the Professor of Internet Governance and Regulation at Oxford University and author of the acclaimed book 'Big Data' shares this view.

"In essence, too much of a comprehensive digital memory might make it almost impossible for us to see the forest, we might only be able to see the trees and that makes it hard for us to take decisions in the present because we are always remembering the decisions of the past.

"In that sense, forgetting plays a very important role," said Mayer-Schoenberger, an Austrian who while living in his home city of Vienna lost ten years of correspondence, when two of his hard drives failed.

"For two days I was crying, I was very depressed and then I just got up and got on with things and it really had no impact on me."

However the data that we have allowed to be collected on our habits and preferences does impact on us. It means that for the first time we have allowed both companies and governments to enter our intimate personal worlds on a systematic and continual basis – despite repeated proof that both types of organisation are untrustworthy.

The result is the collection of huge amounts of data on us, which is then combined with other information that we cannot control or destroy.

For example, Google has laid claim to the exterior views of our homes and can now unite them with other information about us. So Google is effectively populating the street with the sort of information that in the past was only available to our neighbours. This forms part of the identification services that are now being offered by companies like Google, and now Google is laying claim to our bodies too.

According to Professor Fred Cate, a Distinguished Professor at the Indiana University Maurer School of Law and a privacy expert, the amount of data that has been collected on us just via CCTV cameras is alarming because the potential now exists to mine through it using sophisticated algorithms that can track our every move.

"That type of data was collected in a world in which we thought the usefulness of the data was limited. If I didn't see a crime being committed, the data was otherwise going to have no value at all. Today, with facial recognition technology and gait recognition technology there's an ability to match data that frankly we didn't have even two years ago, so those visual images now have all sorts of new

life and new uses," said Cate, who is in a position to know: he is also a member of the US Department of Homeland Security's Data Privacy and Integrity Committee Cybersecurity and the Subcommittee the Department of Defense Advanced Research Projects Agency Privacy Oversight Board.

Professor Cate thinks this means that we should delete CCTV and start again: "Either we should start over – or we need some sort of notification system, so that individuals and groups as well aren't being unfairly discriminated against."

That risk is all too real: currently politicians and the public erroneously believe that surveillance and data monitoring are a panacea for crime and terrorism. According to Mayer-Schoenberger criminal data is considered by many in society to be fair game for retention.

"In the US, state penitentiary departments sell mug shots of prisoners to whoever is prepared to pay a certain price and a company bought hundreds of thousands of them from past prisoners and put them on websites.

"The company who provides this 'service' is actually offering the possibility of taking the name off the website against a hefty fee.

"So in that sense it is blackmail – I have no other word for it – of those who are trying to re-socialise themselves, trying to reintegrate themselves in society."

This effectively means that the technology is now undermining central tenets of our society, the right to forgiveness.

Now the police in the UK and the US are developing systems that will use criminal profiles to find people who are likely to become criminals.

"The problem is that if we do that then we don't know for sure whether or not a person would actually have committed the crime because every prediction based on big data is probabilistic, it's based on probabilities," Mayer-Schoenberger continues.

"Even if there is a 90 per cent chance that I would commit a murder in the next 48 hours, in one out of ten cases I would be sent to prison even though I might not have committed that murder and that I would have put away the knife and walked away from the crime scene.

"There would be a terrible temptation to become involved in a system of predictive social control, a system of social control which slaughters human volition at the altar of collective fear."

Already our lives can now be recorded in great detail. Names and identity can be pinned to the video of our movements. For example, in UK airports, technology monitors the movements of mobile phones to ensure that their owners are behaving in a way that is normal for someone in an airport.

It's a world that is a long way away from the tidal wave that swept away Mustafa and Rina's former lives. They were fortunately re-united and have decided that in the event of it happening again that they will both go to a meeting place only known to them, so they will never get lost again.
Now, with new technology, they probably will not need to do that. Their extended minds will be returned to them and they will be able to meet virtually. But, in return for the service, they will have sold their lives to people who might not have their best interests at heart.

WE ARE SELLING OURSELVES, OUR BIRTHRIGHT, FOR A MESS OF POTAGE.

“IF PRIVACY IS OUTLAWED, ONLY OUTLAWS WILL HAVE PRIVACY.”

Philip Zimmermann, creator of PGP

We're not under the illusion that this document will enforce these principles overnight. But we are confident that this document will help in spreading awareness, in substantiating demands made again and again by the people, and in setting an example for other companies.

EVERY VOICE COUNTS.

If you are an industry or government spokesperson, a startup founder, a blogger, or simply someone with an affinity for privacy and data collection issues, net neutrality discourse or human rights affairs, we would be happy to have your support.

SPREAD THE WORD, MAKE THE PRINCIPLES OF THIS DOCUMENT YOUR OWN.

PX – License and Thanks

Thanks to (in no particular order):

Cory Doctorow, Ewen MacAskill, Peter Warren, Mike Harris and

@mikko_represent @MikeAnnau @GiaFH @GeorgiosZaltos @D3V0M4N @tomsolje @SandraProske @JasonStattler @m_marjaana @boostpublic @mkhiani @klauspeukert @mjormakka @CodesixNET @OllilaAntti @shamrin @damuella @micke_fi @gkweb76 @Afiliali @hki007 @gmoszkow @turtlemantwitt @lavaboomhq @KooCeeFI @virtari @edmurillo17 @anttijarventaus @shaolinturbo @Asiantuntija_69 @ktoro @WilleMiljas @agscotty @MarkoSalmela @TMNIrish @kukaesko @DiabolikKant