RUNNYMEDE GAZETTE

A Journal of the Democratic Resistance

AUGUST 2014

CONTENTS

EDITORIAL

HOW TO BECOME A SQUEAKING WHEEL

BLOCKCHAIN RESISTANCE?

INFORMATION SECURITY FOR JOURNALISTS
Silkie Carlo and Arjen Kamphuis; via Dave Barnby

BIG BROTHER WATCH
Emma Carr

SCOURGE OF SUPERMARKETS
Mike Clayton

WITHDRAW YOUR CONSENT: 25 WAYS TO DECLARE YOUR INDEPENDENCE
Daisy Luther; Activist Post

THE BERNAYSIAN MANIPULATION OF THE HUMAN PSYCHE
Steven MacMillan; Activist Post

THE COMING DIGITAL ANARCHY
Matthew Sparkes; Deputy Head of Technology; Daily Telegraph; via Thomas H Greco

HACKING ONLINE POLLS AND OTHER WAYS BRITISH SPIES SEEK TO CONTROL THE INTERNET
Glenn Greenwald; via Dave Barnby

UEFI - THE MICROSOFT NSA KILL SWITCH
Judy Hope; BCG Bulletin

WHY ARE TBTF BANKS SO HAPPY WITH THE EU BANKING UNION?
Don Quijones; Wolf Street; via Critical Thinking. freecriticalthinking.org.

PARASITE #1: THE SHADOW BANKING SYSTEM
Ellen Brown; Occupy.com; Web of Debt

POSITIVE MONEY BULLETIN
Positive Money Team

EDITORIAL

HOW TO BECOME A SQUEAKING WHEEL

Mike Clayton's brief item on the Scourge of the Supermarkets, gives some ideas on how to make resistance part of daily life, and that to do so is not so difficult.

In the following Activist Post item from Daisy Luther, more flesh is put on this bone. Although written (again!) in the American context, any one of her complaints about overbearing and tyrannical government (in the broadest sense of that term; the oligarchs *are* the government) could apply on this side of the Pond. Again she talks of resistance, not in terms of grand gestures, but of becoming a 'squeaking wheel' … of small daily personal acts of independence and self sufficiency.

And 'protest' is mostly about gesture rather than substance. 'Protest' has been flogged to death by too many over too many years to have much beyond a small impact. It has become the ritual of those whose minds run along tramlines and who either cannot or will not think of anything better to do. It has become a cliché. All demonstrations and other forms of street activity mostly achieve is to offer hostages to fortune and to annoy people.

Resistance is a different animal altogether. It is all about the withdrawal of consent, of realising … as has been argued before in these columns … that we live in an occupied state and must behave accordingly. It is about perceiving 'issues' not as isolated and disconnected phenomena, but as the intimately connected consequences of an oligarchic system.

It is about 'joining hands' and mutual co-operation and co-ordination. It is about organising to put as many fleas on the elephant as possible.

BLOCKCHAIN RESISTANCE?

In its five years (is it really that long!) the *Runnymede Gazette* has often advocated the formation of a cellular resistance network as the only possible mechanism of hurling back the tentacles of oligarchy.

At least and at last there seems to some tentative measure of agreement that something along these line should happen. However, little of practical use has so far been achieved. The question is ... how bad do things have to get,, before sleeves are rolled up in a really serious effort to get things moving? And, by then, will it be too late? We persevere!

A few squeaking wheels will attract little attention, especially if their efforts are

scattered and uncoordinated. What is needed is an entire army of squeaking wheels.

One essential feature of this network model is that it must be entirely decentralised. No national executives; no central committees.

In a fascinating and seminal article in, of all places, The *Daily Telegraph,* Matthew Sparkes paints a vivid picture of a decentralised future, run by systems which are not only decentralised but where, on the Bitcoin Blockchain model, *it is impossible* for any central agency to take control.

I am not a mathematician and do not pretend to understand the mechanics of Bitcoin or Blockchain. But the implications for future political organisation are clear and quite staggering.

Provided the elements of a resistance network are local and autonomous on the one hand, but with well oiled communication networks on the other, the co-ordination aspect will tend to fall into place without the need for any central committee. More than that, the exercise of authority (bearing in mind the difference between leadership and authority ... a leader can only urge and has no power of command) becomes all but impossible.

What has been advocated for a long time in these columns at last has a name.

Frank Taylor

INFORMATION SECURITY FOR JOURNALISTS

Silkie Carlo and Arjen Kamphuis; via Dave Barnby

(This document is far too long to reproduce here. It is also far to important to ignore. These preliminary excerpts give a taste of the subject matter. Although aimed at 'investigative journalists' this may be a cover to forestall allegations of 'promoting terrorism'. Oddly, copies vanished from the internet (quelle surprise!), but I have a copy to forward for anyone interested - Ed)

This handbook is a very important practical tool for journalists. And it is of particular importance to investigative reporters. For the first time journalists are now aware that virtually every electronic communication we make or receive is being recorded, stored and subject to analysis and action. As this surveillance is being conducted in secret, without scrutiny, transparency or any realistic form of accountability, our sources, our stories and our professional work itself is under threat.

After Snowden's disclosures we know that there are real safeguards and real counter measures available. The CIJ's latest handbook, Information Security For Journalists, lays out the most effective means of keeping your work private and safe from spying. It explains how to write safely, how to think about security and how to safely receive, store and send information that a government or powerful corporation may be keen for you not to know, to have or to share. To ensure your privacy and the safety of your sources, Information Security For Journalists will help you to make your communications indecipherable, untraceable and anonymous.

Although this handbook is largely about how to use your computer, you don't need to have a computer science degree to use it. Its authors, and the experts advising the project are ensuring its practical accuracy and usability, and work with the latest

technology.

Gavin MacFadyen, Director of the Centre for Investigative Journalism

Introduction

Imagine opening your inbox to find an anonymous email from someone offering to share important, sensitive documents of international significance with you. The source, and the information, requires the highest level of protection. What do you do?

This manual is designed to instruct journalists and media organisations on how to practise information security in the digital age, protecting your work, your sources, and your communications at a variety of risk levels.

Information security, or "infosec", is the practice of defending information from unauthorized access. The information at stake may include a news report you are working on and any associated files, the identity of your source(s), your communication with them, and at times, your own identity.

You don't need to be an I.T. expert to practise infosec (although you will certainly learn a lot as you go along!). Using this manual, you could find yourself sending encrypted mail and documents from your own highly secure laptop within days!

The Threats: Who Poses a Threat?

Targeted threats

The Snowden revelations have exposed the extraordinary abilities of certain government intelligence agencies to intercept communications, and gain unauthorized access to data on almost any personal computer or electronic communication device in the world. This could pose an information security risk to investigative journalists working on stories concerning the interests of those governments, their agencies, and their private intelligence contractors. Many states lack these sophisticated surveillance technologies – but all states do possess surveillance capabilities, some of which can be, and at times have been, used against journalists, with potentially severe consequences. Ethiopia, a less technologically advanced state, is alleged to have launched remote attacks against journalists stationed in US offices.

In the globalized age, some transnational corporations have greater wealth and power than many sovereign nation states. Correspondingly, some transnational corporations possess greater 'security' or surveillance capabilities than many nation states.

It is not only corporations, but sophisticated criminal organisations that have also been known to employ impressive surveillance technologies – and some criminal organisations may overlap with criminal elements in government. The Mexican army spent $350 million on surveillance tools between 2011 - 2012, and reportedly now possess technologies to collect text messages, phone calls and emails; to remotely automate audio recording on mobile phones; and even to detect movement through walls using radar technology. Also between 2011--2012, 9 journalists were killed in Mexico in association with their work.

Unauthorised access to your data may entail its use, disclosure, disruption, modification, inspection, recording or destruction. You and your source could invoke legal or physical risks, and the information at the heart of your story could be compromised. In high risk situations, infosec may be as important as wearing a bullet--proof vest and travelling with bodyguards. However, because digital threats are invisible, complex and often undetectable they tend to be overlooked.

Dragnet threats

You may also wish to protect yourself from 'dragnet' surveillance programs, led by the US National Security Agency (NSA) and the UK Government

Communications Headquarters (GCHQ).

These are programs that sift through and collect the world's online and telecommunication data - potentially enabling "retroactive investigation." Should you become a person of interest to the government, for example through reporting of secret or controversial state activities, it would be possible to compile a record of your daily activity going back, under current law, as far as five or more years.

Practising Infosec

As an effective journalist, you may find yourself disturbing a few hornets' nests in the course of your career. Practising good infosec therefore means not only employing case-by-case protection strategies, but normalising several permanent strategies that easily fit into your everyday life. However, you will need to use stronger and more effortful infosec methods when working on sensitive topics, and with vulnerable sources.

The first step to practising good infosec is to be aware of the threats; the second, is to be aware of your hardware and software vulnerabilities. Understanding how and why unauthorized access happens is the first step in learning how to protect yourself from it. The threats will change, with time – but so too will the technologies available to protect journalists and citizens. So, it is important to understand infosec in theory, and to always continue learning about infosec in practice.

BIG BROTHER WATCH

Emma Carr

There's No Such Thing As Free WiFi

Following York Council's announcement that the city is to become the first in the UK with city-wide free Wifi, the Council has found itself in hot water for failing to properly inform users about the fact mobile users could find personal information, including their precise location, exposed.

It has been reported that when mobile users sign up for the free WiFi service they are inadvertently handing over vast amounts of personal information. The technology picks up signals from your mobile and links them with your social media profile on your smartphone – storing information such as your age, gender, interests, friends and your location.

Whilst we have become accustomed to accessing internet services for free in the expectation that our data will be used for marketing or advertising purposes (there is no such thing as a free lunch after all), we continue to call for internet users to be provided more transparent information about what happens to their data when they sign up for a service.

Problems of Social Media Law Dismissed

The legislation that governs the use of social media is "generally appropriate", or so says a report from the House of Lords Communications Committee. This is despite the legislation being passed, almost without exception, before social media sites such as Facebook and Twitter were launched.

In its report (PDF) the Committee found that social media law was "generally appropriate for the prosecution of offenses committed using the social media". Yet with a host of cases that many believe should have never even led to arrest never mind to court, we find it concerning that this conclusion has been reached. As it stands, laws that now govern the use of platforms such as Twitter and Facebook,

such as the Malicious Communications Act 1988, were drafted with the intention of combating traditional communications, like threatening phone calls.

SCOURGE OF SUPERMARKETS

Mike Clayton

Chap selling bread (quality) at car boot today said he had rubbish day yesterday because where he normally sells bread at market garden they have just put a tescos supermarket, thus affecting the small traders!

Another chap has said that his mate is selling loads on ebay. I used to but have since stopped.

Both supermarkets, paypal, ebay etc are all involved with the push towards a cashless society (don't forget to link your nectar card in to ebay....). Every transaction will be monitored and recorded. The nation is slowly being dragged into this, mostly unknown. Boycotting these corporations and using cash always and helping the little traders is the best way to resist. Use your hard earned money wisely. You don't need to buy produce from a supermarket because its all glitzy and shiny (that in reality has been stored for a year in a warehouse/chiller and has little nutritional value). Instead buy fresh produce from markets, car boot sales, people selling their home grown produce etc outside their homes. A lot of car boots I go to the little old ladies sell their homemade cakes with decent ingredients and they taste great and have no preservatives/poison in them! The old blokes sell decent quality english tools so you don't need cheap chinese imports that break after 12mths warranty is up. It is easy once you get into it. Start growing your own food/trading with others. I spend £50/mth on food. There is a better way to live outside of their controlled system.

If you keep using the supermarkets etc, then you are only funding your childrens'/ grand childrens' eventually total slavery.

What are you doing to resist?

It is up to you now. I know. Some are already doing this/have started. Everyone can have a go and go back to how we used to live one step at a time.

WITHDRAW YOUR CONSENT: 25 WAYS TO DECLARE YOUR INDEPENDENCE

Daisy Luther; Activist Post

Most of the citizens of the United States are now like the victims of an abusive relationship. People try frantically to avoid breaking laws because they don’t want to be penalized. They sacrifice their own well-being and happiness in order to avoid getting into trouble. I know that I personally get a little burst of adrenaline and say, “Oh crap!” every time a police car happens to be behind me, and I drive a little more carefully, signal a little bit sooner, and make certain my full stop lasts for a count of 5 Mississippis. Our right to defend ourselves with firearms is at risk, you can’t grow vegetables in your front yard in many places, and in some states, you aren’t even allowed to collect the gift of rain to water your garden in dry times. The vast quantity of ever-multiplying statutes are so plentiful even the most law-abiding citizen cannot get through a day without unwittingly breaking one.

"If the laws be so voluminous that they cannot be read, or so incoherent that they cannot be understood; if they be repealed or revised before they are promulgated, or undergo such incessant changes that no man, who knows what the law is to-day, can guess what it will be to-morrow. Law is defined to be a rule of action; but how can that be a rule, which is little known, and less fixed?"

James Madison, Federalist Papers 62

This morning when I was doing my usual rounds of blogs and news, I stopped over at the Mom with a Prep blog, where Jane had published the transcript of the Declaration of Independence as a reminder of why we are celebrating today. The words seemed even more meaningful, considering our current administration, the unjust taxes being forced upon us through Obamacare, and the militarized police force in pretty much every city in America. This section in particular spoke to me:

"We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.–That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed, –That whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it, and to institute new Government, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their Safety and Happiness. Prudence, indeed, will dictate that Governments long established should not be changed for light and transient causes; and accordingly all experience hath shewn, that mankind are more disposed to suffer, while evils are sufferable, than to right themselves by abolishing the forms to which they are accustomed. But when a long train of abuses and usurpations, pursuing invariably the same Object evinces a design to reduce them under absolute Despotism, it is their right, it is their duty, to throw off such Government, and to provide new Guards for their future security."

Our government has crossed the line and become tyrannical. Through insidious acts of terror inflicted upon their own people, they've enacted terrifying, sweeping legislation that give them almost unlimited power…the NDAA (indefinite detention) and the ironically named "Patriot Act", to name two. Law enforcement is just a gang with badges, serving the government and not the people. The "authorities" are running amok, blowing up babies in their cribs and killing homeless people and family pets because they know they'll get away with it. They are nothing but revenue generators, looking for the smallest infraction for which to fine you.

We can't afford to help the hundreds of thousands of Americans in Detroit who have lost their running water, but we can invite hundreds of thousands of immigrants to just walk on in, and we can afford to house them, feed them, give them medical care, and transport them throughout our country. And it isn't just enormous things like Obamacare, immigration, gun control, and indefinite detention.

It's everyday things that allow us to be self-sufficient and independent from "the system" that are becoming outlawed. What on earth has our nation come to, when growing your own food is an act of revolution? When being armed in order to defend yourself and your family is considered some kind of subversive act? When the public schools, which used to teach useful things like Home Economics and Auto Shop, and used to have extracurricular sports like marksmanship, now suspend children for pointing their fingers and saying "bang"? When collecting a bounty of rainwater for dry times is against the law?

How is it acceptable that the government can attempt to force people to inject toxins (in the form of mandatory vaccines) into our bodies and our children's bodies? How is it acceptable that they can attempt to force us to send our children to approved schools to learn approved curricula? That they force us to pay each year in order to drive our cars and live in our paid-for homes?

I'm pretty sure this is what our forefathers meant when they said "But when a long train of abuses and usurpations, pursuing invariably the same Object evinces a design to reduce them under absolute Despotism, it is their right, it is their duty, to throw off such Government, and to provide new Guards for their future security."

The 13th Amendment to the Constitution abolished slavery. This means that if you are a slave today, it's either illegal, or you have voluntarily accepted your servitude.

"*Neither slavery nor involuntary servitude, except as a punishment for crime whereof the party shall have been duly convicted, shall exist within the United States, or any place subject to their jurisdiction.*"

You have a Constitutionally protected right to be free. If you aren't free, then revolution is your duty. Part of the power that the government holds over people is the fact that they have stuff we need. So, the key to independence is not to need the stuff they have. When there is nothing that you require enough to submit, then bullying you becomes much more difficult. Here are some examples:

If you reduce your consumerist habits and lower your cost of living, you need less money.
If you grow your own food, you will never be dependent on the government to help you to afford to buy food.
If you don't send your kids to school, and instead educate them at home, then you don't need to get them vaccinated so they can attend school.
If you don't make much money, you don't pay much in the way of taxes.
If you are self-employed, you can't be threatened with the loss of your job for non-compliance with *pick a ridiculous law.*
If you shop locally, from farms and craftsmen, you don't need the big box stores.
If you have the ability and equipment to defend yourself, you don't need to call 911.

This isn't about guns blazing, militias mobilizing, and guerilla warfare. It's about small personal acts of independence. The way you lead your life every single day can be a personal Declaration of Independence. By refusing to concede your natural rights, quietly and resolutely, you are performing an act of revolution. This only requires your consistent determination not to be infringed upon.

Personally, I withdraw my consent to be governed by the people in Washington DC that allegedly represent me. Because they don't. They do not mirror my wishes and beliefs. They do not support my pursuit of personal freedom.

The most revolutionary act is to be self-sufficient and in need of nothing that the government can provide for you in exchange for some small liberty. This list of insurrections is by no means comprehensive.

1. Question absolutely everything you hear on the news. Always be a skeptic. All major media goes back to just a few conglomerates The "news" is now all a propaganda ploy to help the rich get richer and the powerful remain in power. The media can make or break a candidate with unholy zeal in less than a week. These people and others like them are the ones that decide what "we the people" get to see. If they feel like a candidate or a news item might upset the status quo, they black it out by refusing to cover it.

2. Call out the media. Let everyone know that the mainstream media is the enemy of the people. When you see coverage that is clearly biased, take a moment to call out the media about it. Take the time to comment on mainstream media websites and point out the unbalanced coverage. If you use social media, share this information and post on the media outlet's social media pages as well.

3. Get out of the banking system. By opting to "unbank" or "underbank" there is a limit to what can be easily stolen from you. When you have physical control of your financial assets, you are not at as high a risk of losing those assets, and therefore, less likely to be dependent on "the system."

4. Turn your savings into precious metals or tangible assets. On the same note as unbanking, you definitely don't want to rely on a 401K or savings account to provide for you in your old age. Ask

the people of Cyprus how well that worked out for them. Diversify with assets you can touch. Purchase tangible goods like land, food, ammo, and seeds. Once you are well supplied, move on to precious metals to preserve your wealth.

5. Educate others. At the (very high) risk of people thinking you're crazy, it's important to let people know WHY you do what you do. If you are an anti-Monsanto activist, teach others about the dangers of GMOs. If you object to a municipal policy, speak at a town meeting or send a letter to the editor of your local paper. By ranting incoherently or by keeping your mouth shut, you influence no one. By providing provable facts, you can open minds and awaken others to tyranny.

6. Get others involved in the fight. For example, if you are fighting with the city council that wants to rip out the vegetables growing in your front yard, let your friends and neighbours know, post a notice at the grocery store, and write a letter to the editor. When injustice occurs, use the power of social media to spread awareness. Often a public outcry is what is necessary to get the "authorities" to back down. Look at the case of Brandon Raub, the veteran who was kidnapped and taken to a mental hospital for things he posted on Facebook. Raub was not charged, but he was detained in the psych ward involuntarily. His friends and family immediately mobilized and spread the videos of his arrest all over the Internet. It snowballed and alternative media picked it up – soon Raub was released, and all because of a grass roots and social media campaign to bring the injustice to light.

7. Grow your own food. Every single seed that you plant is a revolutionary act. Every bit of food that you don't have to purchase from the grocery store is a battle cry for your personal independence. When you educate yourself (and others) about Big Food, Big Agri, and the food safety sell-outs at the FDA, you will clearly see that we are alone in our fight for healthy, nutritious foods. Refuse to tolerate these attacks on our health and our lifestyles. Refuse to be held subject to Agenda 21's version of "sustainability".

8. Take control of your health. It is imperative that you not blindly trust in the medical establishment. Many members of this establishment are merely prostitutes for their pimp, Big Pharma. Millions of children are given powerful psychotropic drugs to help them fit into the neat little classroom boxes, and the numbers are growing every day. Americans spent 34.2 BILLION dollars on psychiatric drugs in 2010. (Source) Big Pharma is an enormously profitable industry that only pays off if they can convince you that you're sick. Learn about the toxic injections and medications, weight the risks and benefits, and always look for second and third opinions before making a medical decision. Maintain your health by avoiding toxins, exercising, and ditching your bad habits to reduce the number of doctor's visits that are necessary.

9. Refuse to comply. If you know your natural rights, which are guaranteed under the Constitution and its Amendments, then it makes it much harder for "authorities" to bully you. You don't have to let them search your home without a warrant, you don't have to answer questions, and you don't have to comply with laws that are in conflict with the Constitution.

10. Don't overlook the little things. Governments like to chip away at rights a tiny bit at a time, until one day you wake up and realize that all of those little things add up to a really big deal. Today, the bulk purchase of ammo might limited. Tomorrow, you might not be able to buy it at all. Today, home births might be subject to a set of rules. Tomorrow, those rules might be expanded to the point that the birth of your child is totally legislated.

11. Learn. Every day, spend time learning. This shouldn't stop once our formal education ends. Fill your mind with history, with current events, with constitutional law, and information about the natural world. Learn about health, study economics, research things that interest you, and unravel

the complicated conspiracies that are afoot. To pursue unbiased knowledge is to free your mind from the prison of propaganda and indoctrination.

12. Don't consume chemicals that cause you to be dumbed down. Avoid chemical-laden food with brain-killing neurotoxins like MSG and aspartame. Don't drink fluoridated water.

13. Embrace your right to bear arms. Be responsible for your own safety and security.

14. Don't be in debt. No one can be free if they are in debt. If you are in debt, you are forced to work in whatever conditions are present, for whatever amount is offered, complying with whatever criteria is necessary to keep your job in order to either pay your debt or face penalties. As well, the high interest rates that you pay only serve to make the bankers more wealthy. Instead of borrowing, save until you can afford something or realize that if you could actually afford it, you wouldn't need to borrow money to have it.

15. Be prepared for disaster. Have enough food, water, and supplies to take care of your family in the event of a natural disaster. Don't expect FEMA to take care of you.

16. Be involved in your children's education. For some, this means home-schooling or unschooling, and for others this means being on top of what they are learning in a formal school setting. Join the PTA and actively volunteer if your child goes to school. Be an advocate for your child and insist that the teachers teach. If your child goes to school, supplement this at home with discourse about current events and outings that help them learn about the world around them.

17. Be the squeaky wheel. If you see something wrong, don't just ignore it. Say something about it, and keep saying something until it changes. Whether this is some process that infringes on your privacy, a job requirement that impedes your health, or another injustice, pursue it relentlessly. Ask questions publicly, write letters, and use social media to bring pressure to encourage a change.

18. Reduce your consumer spending. Spending less helps to starve the beast by reducing the sales taxes you pay and withdrawing your financial support to big conglomerates. If we vote with our dollars, eventually there will, of a necessity, be a paradigm shift that returns us to simpler days, when families that were willing to work hard could make a living without selling their souls to the corporate monoliths. A low-consumption lifestyle reduces your financial dependency, which allows for more freedom.

19. Ditch popular culture. If reality TV isn't a tool for dumbing people down, I don't know what it is. My daughter recently begged to watch an episode of a popular reality TV show that "everyone" was watching. She managed about 15 minutes of it and then said, "This is the stupidest thing I've ever seen." She decided to read a book instead. Popular entertainment is a media tool used to change our perspectives about our personal values, and to tell us how to think and feel about issues.

20. Buy locally. Support local small businesses to help others who are fighting for independence from the system. You might pay a little bit more than you would at your big box store, but the only people benefiting from your purchases made at the corporate stores are those with the 7-figure annual bonuses.

21. Develop multiple streams of income. Don't put all of your eggs in one basket. Figure out several ways to bring in income. Not only does this free you from being a wage slave, but it allows you to hire friends or family members. You are less entangled in the system and not subject to corporate whims. If one business fails, or becomes subject to regulations that make it no longer

worthwhile, you are not forced to comply just to keep a roof over your head. (Learn more HERE)

22. Say thanks, but no thanks. There is no such thing as a benevolent hand out. Nearly anything offered for free (particularly by a government entity) has strings attached. Maybe there is a handy-dandy registration form that you need to fill out. You might be influenced to vote a certain way just to keep the freebies coming. You might have to pee in a cup every two weeks. Perhaps one day you'll need to have a microchip embedded in your hand. Either way, by accepting handouts from those in "authority", you become beholden to them or you need them, and someone who is free is neither beholden nor needy.

23. Collect water. Either harvest it with rain barrels, store it in a cistern, or create a source for it on your property (digging a well, for example.) Water is life.

24. Don't take the easy road. The PTB like to seduce people with simplicity. "If you just sign this paper, it will be much easier," they say. "This chip is for your convenience," they tell you. "By giving up this, it lets us take care of you and you will be much safer." The easy road only gets you to Slave Street a whole lot faster. Take the difficult road and be responsible for yourself. Don't take shortcuts that compromise your beliefs. Go to court to fight a ticket, read the laws and defend yourself.

25. Know that anything you give up, you will never get back.

Today, to celebrate Independence Day, I'm taking another small step to free myself from their system. I'm revolting by beginning construction on a chicken coop. I'm declaring my own independence by making my small town home as self-sufficient as possible.

How will you revolt against tyranny today?

Daisy Luther is a freelance writer and editor. Her website, The Organic Prepper, where this article first appeared, offers information on healthy prepping, including premium nutritional choices, general wellness and non-tech solutions. You can follow Daisy on Facebook and Twitter, and you can email her at daisy@theorganicprepper.ca

THE BERNAYSIAN MANIPULATION OF THE HUMAN PSYCHE

Steven MacMillan; Activist Post

Edward Bernays was the master of influencing and shaping public opinion who developed upon the ideas of earlier social psychologists and the work of his uncle, Sigmund Freud, in order to create techniques to manipulate the subconscious desires of the masses.

Throughout his 103-year lifespan, the "father of public relations" was at the pinnacle of his field advising US Presidents Coolidge, Eisenhower, Hoover and Wilson, as well as inventor Thomas Edison, US industrialist Henry Ford and First Lady Eleanor Roosevelt. He also reportedly refused invitations by Hitler and Franco to work on fascist propaganda campaigns in Europe.

At the end of World War 1 Bernays served as a propagandist for America before going on to work with various government departments and corporations throughout his lifetime, including: the US Department of State, CBS, Procter and Gamble, and the American Tobacco Company, as well as designing the propaganda campaign for the United Fruit Company which led to the CIA coup against the Guatemalan President Jacobo Árbenz in 1954.

Bernays combined the work of people such as the French social psychologist Gustave Le Bon to create techniques which appeal to the subconscious emotions of the public, as opposed to engaging the public in rational and intellectual debate. Le Bon studied the mental characteristics and the behaviour of the crowd, believing that when part of a mass, individuals are subordinate to the crowd mind and that a human behaves in a more emotive, irrational manner. Bernays observed that if a propagandist could understand the "motives of the group mind", they would possess the ability to

“control and regiment the masses”:

"*The systematic study of mass psychology revealed to students the potentialities of invisible government of society by the manipulation of the motives which actuate man in the group. Trotter and Le Bon, who approached the subject in a scientific manner, and Graham Wallas, Walter Lippmann, and others who continued with searching studies of the group mind, established that the group has mental characteristics distinct from those of the individual, and is motivated by impulses and emotions which cannot be explained on the basis of what we know of individual psychology. So the question naturally arose: If we understand the mechanism and the motives of the group mind, is it not possible to control and regiment the masses according to our will without their knowing of it?*”

(Bernays, 1928, p.71)

Bernays continues to reveal the growing ability of the propagandist to understand and successfully alter “public opinion” way back in the 1920s, long before television sets were in every household and the sophisticated modern media techniques of today:

"*The recent practice of propaganda has proved that it is possible, at least up to a certain point and within certain limits. Mass psychology is as yet far from being an exact science and the mysteries of human motivation are by no means all revealed. But at least theory and practice have combined with sufficient success to permit us to know that in certain cases we can effect some change in public opinion with a fair degree of accuracy by operating a certain mechanism, just as the motorist can regulate the speed of a car by manipulating the flow of gasoline.*"

(Bernays, 1928, p.71 & p.72)

The basic premise of Bernays thesis is that humans are “rarely aware” of the true motivations ad desires powering their actions, and if certain individuals could uncover the real desires of the mass mind, the public could be influenced and manipulated without their knowledge of it:

"*Men are rarely aware of the real reasons which motivate their actions . . . It is chiefly the psychologists of the school of Freud who have pointed out that many of man’s thoughts and actions are compensatory substitutes for desires which has been obliged to suppress. A thing may be desired not for its intrinsic worth or usefulness, but because he has unconsciously come to see it as a symbol of something else, the desire for which he is ashamed to admit to himself…. This general principle, that men are very largely actuated by motives which they conceal from themselves, is as true of mass as of individual psychology. It is evident that the successful propagandist must understand the true motives and not be content to accept the reasons which men give for what they do . . . Human desires are the steam which makes the social machine work. Only by understanding them can the propagandist control that loose-jointed mechanism which is modern society.*"

(Bernays, 1928, p. 74, p.75 & p.76)

The study of mass psychology and herd behaviour were important areas which had to be understood to intelligently manipulate the public:

"*The whole basis of successful propaganda is to have an objective and then to endeavour to arrive at it through an exact knowledge of the public and modifying circumstances to manipulate and sway that public*."

(Bernays, 1928, p.126)

"*But clearly it is the intelligent minorities which need to make use propaganda continuously and systematically . . . Small groups of persons can, and do, make the rest of us think what they please about a given subject*"

Bernays, 1928, p.57)

In ancient times, leaders of a tribe, group or society processed tremendous power over the rest of the people especially if they are skilled in the art of persuasion. Political leaders in modern times have the ability to shape and mould the psychology of their followers in a truly profound manner, especially if they have the ability to use propaganda effectively:

"*The voice of the people expresses the mind of the people, and that mind is made up for it by the group leaders in whom it believes and by those persons who understand the manipulation of public opinion. Fortunately, the sincere and gifted politician is able, by the instrument of propaganda, to mould and form the will of the people.*"

(Bernays, 1928, p. 109)

Bernays reveals the power propagandists have to manipulate and control the "public mind" through understanding the techniques of managing the public:

"*The conscious and intelligent manipulation of the organised habits and opinions of the masses is an important element in democratic society. Those who manipulate this unseen mechanism of society constitute an invisible government which is the true ruling power of our country. We are governed, our minds moulded, our tastes formed, our ideas suggested, largely by men we have never heard of . . . Whatever attitude one chooses toward this condition, it remains a fact that in almost every act of our daily lives, whether in the sphere of politics or business, in our social conduct or our ethical thinking, we are dominated by a relatively small number of persons – a trifling fraction of our hundred and twenty million – who understand the mental processes and social patterns of the masses. It is they who pull the wires which control the public mind, who harness old social forces and contrive new ways to bind and guide the world*"

(Bernays, 1928, p.37 & p.38)

Sources: Edward Bernays – Propaganda 1928

Steven MacMillan is a Scottish researcher and writer who founded The Analyst Report, where this article first appeared.

THE COMING DIGITAL ANARCHY

Matthew Sparkes; Deputy Head of Technology; Daily Telegraph; via Thomas H Greco

Bitcoin is giving banks a run for their money. Now the same technology threatens to eradicate social networks, stock markets, even national governments. Are we heading towards an anarchic future where centralised power of any kind will dissolve? The same technology that powers Bitcoin can be harnessed to disrupt a range of other systems.

The rise and rise of Bitcoin has grabbed the world's attention, yet its devastating potential still isn't widely understood. Yes, we all know it's a digital currency. But the developers who worked on Bitcoin believe that it represents a technological breakthrough that could sweep into obsolescence everything from social networks to stock markets... and even governments. In short, Bitcoin could be the gateway to a coming digital anarchy – "a catalyst for change that creates a new and different world," to quote Jeff Garzik, one of Bitcoin's most prolific developers.

It's already beginning. We used to need banks to keep track of who owned what. Not any more. Bitcoin and its rivals have proved that banks can be replaced with software and clever mathematics. And now programmers of a libertarian bent are starting to ask what else we don't need.

Imagine driverless taxis roaming from city to city in search of the most lucrative fares; a sky dark with hovering drones delivering your shopping or illicit drugs. Digital anarchy could fill your lives and your nightmares with machines that answer to you, your employers, crime syndicates… or no one at all. Nearly every aspect of our lives will be uprooted.

To understand how, we need to grasp the power of the "blockchain" – a peer-to-peer ledger which creates and records agreement on contentious issues with the aid of cryptography.

A blockchain forms the beating heart of Bitcoin. In time, blockchains will power many radical, disruptive technologies that smart people are working on right now.

Until recently, we've needed central bodies – banks, stock markets, governments, police forces – to settle vital questions. Who owns this money? Who controls this company? Who has the right to vote in this election?

Now we have a small piece of pure, incorruptible mathematics enshrined in computer code that will allow people to solve the thorniest problems without reference to "the authorities". The benefits of decentralised systems will be huge: slashed overheads, improved security and (in many circumstances) the removal of the weakest link of all – greedy, corruptible, fallible humans.

But how far will disruptive effects reach? Are we rapidly approaching a singularity where, thanks to

Bitcoin-like tools, centralised power of any kind will seem as archaic as the feudal system? If the internet revolution has taught us anything, it's that when change comes, it comes fast.

Funny money

Let's start with digital currency. Right now, in the wake of an unprecedented financial crisis, it's easy to understand the appeal of a new money that lies beyond the grasp of banks and governments. No treasury can print more Bitcoins and inflate away the value of your savings, or recklessly lend them out for years to people with no chance of meeting repayments, eventually bringing the whole system crashing down. The rules of Bitcoin are set in digital stone.

It all began with a paper written by someone calling himself "Satoshi Nakamoto" and quietly published via a cryptography mailing list in 2008. It laid out a plan for a form of money based on "cryptographic proof instead of trust". Nakamoto described a way of keeping a ledger of all transactions – the blockchain – to prove who owned what. It was a breakthrough which solved a longstanding computer science problem: how to run a complex system with no central control.

Bitcoin has no bank to maintain security, record ownership or handle transactions. None is needed.

The true identity of Satoshi has never been revealed, although rumours abound: a lone academic, a group of disgruntled, anarchist programmers working in the financial sector, the CIA...

What is known is that the number of coins in circulation is finite, limited to 21 million. The plan is immutable: around 13 million are already in existence and the last ones will be released in 20 years or so.

Critics who say Bitcoin is nothing but zeros and ones in a computer file and therefore can't hold value miss the point that their bank balance is, similarly, nothing but a number on a computer.

The pound is worth something only because people decide to place value in it. If that consensus broke down, then – as in Weimar Germany – a wheelbarrow full of £20 notes couldn't buy you a cup of coffee. Sterling is a famously stable currency – but just occasionally we're brought up with a jolt. For example, in 2007 Northern Rock was forced to go cap-in-hand to the Bank of England. A few customers rushed to withdraw their money, then a few more... and soon there was panic. Loss of faith. Shades of Weimar, or even Zimbabwe.

If national currencies can fall victim to a chain-reaction erosion of faith, why should a new currency not experience the same phenomenon in reverse?

Last year Cyprus horrified citizens when it announced that it would seize up to 60 per cent of all savings over €100,000 to save its struggling banks. Suddenly Bitcoin seemed less risky and transaction volumes soared as people poured cash into the digital currency to keep it out of government coffers. This same land grab could not happen with Bitcoin. There is no central power with the ability to skim off the top.

Neither are credit-fuelled binges possible. The smoke-and-mirrors system that banks use to magic money into existence when they create loans is not possible in a Bitcoin world.

This holds a lot of appeal. Financial Times columnist Martin Wolf recently called for banks to be stripped of this bizarre right to create money from thin air, claiming that it was the root cause of credit bubbles and busts such as the painful cycle we have just witnessed. In his view, they should be confined to only lending the amount they have taken as deposits from savers. It's hard to argue against such a commonsense proposal.

It is perhaps no coincidence that Bitcoin emerged from the ashes of a savage recession. Although it is radical in many ways, it is also strictly conservative: no debt is possible, no complex derivatives, no untrustworthy middlemen. You either have coins, or you don't. The timing was impeccable, the perfect antidote to a financial system which can't be trusted not to lead us into another round of boom and bust.

The old order: controlling the internet

The banks aren't the only institutions whose future is threatened. The blockchain has the power to uproot a number of our most recognisable dot coms.

The internet, rife with accidental data leaks like eBay's latest mishap and government eavesdropping, is crying out for anarchic disruption. Lack of trust in banks has become lack of trust in the guardians of cyberspace. There is a growing mood that nobody can be trusted with our money or our data.

We think of the internet as a libertarian free-for-all, a place where anything goes and governments fear

to tread. But nothing could be further from the truth. The Internet was a US invention born out of the Department of Defence in the late 60s, and the American government keeps a firm grip on the reins to this day. In the 90s maintenance of the internet was overseen by just one man: a computer scientist, on the payroll of the Department, called Jon Postel. Once the job outgrew him, the US government set up a nonprofit called the Internet Corporation for Assigned Names and Numbers (ICANN) to take over the task. It now keeps track of who owns which domain names and maintains various systems that underpin the internet and the World Wide Web.

ICANN presents itself as a friendly caretaker and security guard, with an altruistic motto: “One World. One Internet.” It operates under a mandate from the US government to run things in a “bottom up, consensus driven, democratic manner”. Its blog – yes, it has a blog – switches fluently from Silicon Valley gush (“this incredible journey”) to corporate jargon (“a multistakeholder approach to the future evolution of Internet governance”).

Since 2010, ICANN has opened four new offices – in Los Angeles, Washington DC, Brussels and (of course) Silicon Valley. As its website boasts: “The contemporary architecture of all four offices visually expresses ICANN's organisational mandate for transparency through glass office and conference room walls and floor-to-ceiling windows that allow in natural light.” But does ICANN’s operational transparency match that of its gleaming windows?

Its advisory committee of national governments, the World Bank, the World Trade Organisation and Interpol is often criticised for deciding important matters behind closed doors. And the most recent moves towards “transparency” seem designed to achieve the opposite. ICANN wants to restrict access to Whois, a facility that allows anyone to know who has registered a domain name on the internet. Instead, this information would be available to “appropriate” interested parties. Put bluntly, the global machinery of the internet is operated by a conglomerate dominated by governments – and especially the US government.

Also, individual governments around the world have their own censorship tools. The crucial point is that censorship is a spectrum. Few of us would object to the UK’s practice of blocking child pornography – but what about the banning of file-sharing websites? Or the ham-fisted blocking of any information critical of an authoritarian regime?

Meanwhile, largely thanks to Edward Snowden, we’re waking up to the fact that the same governments which restrict what we can see are themselves able to peer into our private lives. Documents leaked by Snowden revealed that the UK’s hi-tech spy agency GCHQ, based in Cheltenham, has captured images from private webcam conversations between people of no interest in any ongoing investigation – "unselected", in their slightly chilling terminology. Over a million webcam users were caught up in this fishing expedition. Many of these images turned out to be sexually explicit. They remain on file in Cheltenham.

The new order: unravelling the internet

America and Britain have the resources to create tools to pull off tricks like these themselves. Smaller countries turn to the private sector, which is only too delighted to help out. And this is where the game changes: from controlling the internet to unravelling it.

Andover is a mildly picturesque market town in Hampshire. It’s an unlikely setting for the offices of Gamma, a controversial internet security company that sells FinFisher, described by Bloomberg as “one of the world’s most elusive cyberweapons, which can secretly take remote control of a computer, copying files, intercepting Skype calls and logging every keystroke”.

In the aftermath of the Arab Spring, the BBC reported that it had seen documents in the looted headquarters of the Egyptian state security building that suggested Gamma software had been used in a five-month trial to target pro-democracy activists. The company denied supplying the software. (It failed to respond to requests for comment when the Telegraph contacted it.)

Gamma's managing director, Martin Muench, is in his early 30s, dresses in black and comes from a small town in north Germany that he won’t name because he fears for his family’s security. He says FinFisher helps captures paedophiles and terrorists, who regard him as “the personified evil”. He’s not popular among human rights activists in Bahrain, either: as Bloomberg reported in detail, they claim FinFisher has been used against them. Muench denies that FinFisher is a tool for tyrants. He’s someone who carefully guards his reputation and his privacy.

Muench and Gamma operate within the law: FinFisher is not an illegal tool, though it can be used

illegally. Tweak the technology a bit, however, and you have something like Blackshades Remote Access Tool (RAT), which is regarded as “malicious commercial software”.

Blackshades RAT was used last year to capture naked photographs of the then 19-year-old Miss Teen USA Cassidy Wolf. Jared James Abrahams, 20, threatened to post the photos online unless Wolf gave him a nude video. He was later sentenced to 18 months in prison. At the end of May this year, nearly 100 people were arrested in a worldwide crackdown on the creators, sellers and users of Blackshades RAT. It’s a hackers’ and blackmailers’ tool. Follow its trail and you’ll soon find yourself in strange places. Police making the Blackshade arrests seized 1,100 data storage devices suspected of being used in illegal activities. They also found stolen cash, guns and drugs.

Organised crime is technology-obsessed. That makes life tough for law enforcement – but it’s also evidence of a wider trend.

Governments and agencies companies which have, until now, had total control over the internet are fast losing it. Like holding a handful of sand: the harder they squeeze, the quicker it slips away.

Here’s an illustration. The University of Abertay in Dundee now offers a four-year BSc in “Ethical Hacking”. Abertay is a minor university and some of its other courses – eg, a BSc in “Performance Golf” – invite ridicule. So, on the face of it, does “Ethical Hacking”, which could mean anything.

According to the prospectus, “the business world is seeing a rapid increase in the demand for ethical or white hat, hackers, employed by companies to find security holes before criminal, black hat, hackers do … Hackers are innately curious and want to pull things apart. They experiment and research. A hacker wants to learn and investigate. The aim is for you to arrive on this programme as a student and leave as an ethical hacker.” Graduates will have state-of-the-art knowledge of penetration testing, cryptography and biometric identity systems. They will be intimately familiar with the habits of “black hat” hackers.

As a result, they will not find it difficult to land well-paid jobs. Many of these jobs could even be inside GCHQ itself. The agency sponsors an annual hacking tournament which attracts thousands of entrants of exactly the kind that The University of Abertay is after, who are whittled down through numerous online rounds to the few dozen who take part in a final and extremely realistic cyber-attack simulation. This year it was held in the Cabinet War Rooms deep beneath Whitehall.

At this year’s event I spoke to a man from Cheltenham who refused to give me his name, who said that “some of the skills you see here today are what GCHQ would be doing”. He was one of many people watching proceedings wearing a special armband whom I was forbidden from photographing. Later, I asked Stephanie Daman, chief executive of the Cyber Security Challenge, how many of the people in the room would be hoovered up by the security agencies, but was told with a smile that such things aren't revealed. But if somebody performed well and then didn’t reappear next year? You can make your own inferences from that, she said: “We’re not a recruitment agency. We provide a place for people to meet.”

Whether these ethical hackers will stay ethical is another question, however.

Social networks, search engines and online retailers have grown rich by soaking up our personal data and distilling it into valuable databases used to surgically target advertising. As the adage goes: “If you’re not paying, then you’re the product”. You don’t pay a penny for Google’s search engine, email or calendar products. What you do provide, though, is data on every aspect of your life: who you know; where you go; what you enjoy eating, wearing, watching.

An unimaginable amount of information is being analysed and exploited by companies in order to screw money out of us. But rather than having to collect it, we are handing it to them in return for a simple, free way to chat to our friends, share pictures or send emails.

Behind the laid-back, let’s-play-table-football facade of Silicon Valley firms lies a sneakiness and paranoia that, critics say, verges on the sociopathic. This is hardly surprising. The giant dotcoms stand to lose billions of dollars and even kick-start a US recession if the internet becomes too unstable for them to manage. But, in addition, they need to take advantage of digital instability in order to shaft their rivals.

“These guys are control freaks who see themselves as ‘disruptive’, to quote one of their favourite words,” says a California-based analyst. “It’s a very combustible mixture particularly when you consider the endless, endless uncertainty they face every day.”

The biggest corporations work overtime to maintain the appearance of omnipotence. Dave Eggers satirises one such firm in his novel The Circle, about a sinister West Coast dotcom whose slogans include “secrets are lies” and “privacy is theft”.

In an interview with McSweeneys, Eggers said he often had to delete sections of his manuscript when

truth caught up with fiction: “A lot of times I’d think of something that a company like the Circle might dream up, something a little creepy, and then I’d read about the exact invention, or even something more extreme, the next day.”

Now we need to put our finger on a really important paradox that lies at the heart of the coming digital anarchy. The hidden power of the Facebooks, Twitters and Googles of this world is inspiring digital anarchists to destroy the smug, jargon-infested giants of Silicon Valley. But who are these hackers? They’re unlikely to be career criminals who identify themselves by their black hats. On the contrary, they may well have picked up their techniques while working in Palo Alto. In some cases, the very same people who helped create these mega-corporations are now working on “disruptive technologies” to replace them.

We think of Silicon Valley as peopled by “liberals”. But that’s misleading. They may be socially liberal, but their “libertarianism” is often predicated on very low taxes funding a very small government. They have a soft spot for the anti-tax Republican Rand Paul and the kill-or-be-killed ethos of the paranoid libertarian capitalist Ayn Rand (whom Mr Paul was not named after, though he’s had to spend his whole life denying it).

The digital utopias at the back of these people’s minds are often startlingly weird. Consider, for example, Peter Thiel, the founder of PayPal – ironically, one of the companies Bitcoin aims to blow out of the water. He has donated $1.25m to the SeaSteading Institute, a group which aims to create an autonomous nation in the ocean, away from existing sovereign laws and free of regulation. At a conference in 2009 he said: "There are quite a lot of people who think it's not possible. That's a good thing. We don't need to really worry about those people very much, because since they don't think it's possible they won't take us very seriously. And they will not actually try to stop us until it's too late."

It’s difficult to generalise about motives when the membranes separating control and anarchy, creativity and disruption, greed and philanthropy have become so alarmingly thin. Remember that the entrepreneurs of Silicon Valley and its many global franchises are usually young enough to be impressionable and excitable. Yes, some of them they may qualify as utopians – but, like utopians throughout history, they are ready to use destructive tactics to reach their goal.

What is that goal? Right now, and put simply, it’s to create what they regard as “incorruptible” versions of the websites, networks and financial institutions which we all rely on every day – to remove the man in the middle and any ulterior motives he may have. The new digital anarchists – who are as likely to wear Gant chinos as hoodies, and wouldn’t be seen dead in an Anonymous mask – are in the mood to punish Facebook, Google, Twitter, PayPal, eBay, you name it, for their arrogance. Indeed, they may have encountered this arrogance close up by working for them. That’s enough of a motive for the great digital unravelling.

As for means and opportunity – well, they now have their weapon of choice: the blockchain. We need to understand more about this concept, so let’s return to Bitcoin and peer beneath the bonnet.

Why the blockchain changes everything

In our current banking system we all have accounts holding certain amounts of money. To pay for a coffee at Starbucks we tell the bank, often via a chip-and-PIN machine, that we’d like to transfer £3. Starbucks’s account balance goes up £3, ours goes down £3, and the bank tallies the books. Bitcoin removes the banker, the man in the middle, who can choose to levy fees, disclose information to governments... or do anything else they see fit which may anger your average libertarian anarchist. (Some of them live in a permanent state of resentment, it should be said.)

But doing so is far from simple. Who tracks how much money everyone has, if not the bank? If it were left to individuals, we would all add a few zeros to our balances and the whole thing would descend into a fraudulent farce.

Bitcoin’s solution is for everyone to record all information. We will all be the bank. As we saw earlier, the blockchain is the public ledger of all transactions, showing how much each person owns, and it is stored by Bitcoin users all over the planet. The clever part is how the network reaches a consensus on what should be written in it. Otherwise there could be thousands of different blockchains, all disagreeing over who owns what.

The idea is that each and every transaction is broadcast by the person initiating it. Rather than telling the bank we want to spend £3, we tell the world. That transaction is bundled up with thousands of others and cryptographically bound into a “block” by “miners”. Technically, anyone with a computer can be a miner

– they just need to install a small piece of software. But it's not easy to do: far from it.

Bitcoin "miners" are so called because gold miners traditionally have to put in a lot of work before they see any reward in the shape of precious metal. In the world of Bitcoin, miners have to crack an extremely difficult cryptographic problem before they are rewarded with some newly minted Bitcoins. That "block" is then added to the end of the blockchain and shared around the world.

To quote the wiki dictionary maintained by "the Bitcoin community" – perhaps the nearest you can get to an official explanation – "mining is intentionally designed to be resource-intensive and difficult so that the number of blocks found each day by miners remains steady … The primary purpose of mining is to allow Bitcoin nodes to reach a secure, tamper-resistant consensus." In other words, the blockchain remains both public and infallible. It's a totally reliable and trustworthy record of who owns what, but also who owned what back through time, all the way to the creation of Bitcoin.

Anyone attempting to alter that ledger to steal a coin would have to re-do all of the difficult calculations that were done to embed it there the last time it was traded. Then they would have to do the same with all the later blocks on top of it up to the current date, and then get far enough ahead that they were the first people to crack the newest block and get it accepted as the definitive version.

In short, it's impossible.

Our first taste of this decentralised power happened to be a currency, Bitcoin, but it could equally have been a stock exchange, a social network or an electronic voting system. Jeff Garzik, the Bitcoin developer, tells me that the blockchain technology is "the biggest thing since the internet – a catalyst for change in all areas of our lives". He's currently fundraising to put Bitcoin satellites into space to rebroadcast the latest version of the blockchain around the world for those without reliable internet connections. That's how strongly he believes in it. "Currency is simply the first application of Bitcoin's decentralised technology," he tells me from his Atlanta home. "Bitcoin is many layers of an onion. Peel back one layer, and a new and amazing layer awaits underneath to discover."

When power is concentrated in the hands of a few powerful people there is a risk of catastrophe, corruption and chaos, he warns. Decentralising a system hands power to immutable mathematics. And then the game really changes. Things fall apart

Remember those luxurious glass offices built by ICANN in order to emphasise its "transparency"? These days an awful lot of anxiety is flooding in along with the sunlight.

ICANN's vice-like grip on domain names is now looking more tenuous than ever before. Currently the group decides which top-level domains can exist (.co.uk for example) and hands out a licence to sell addresses underneath them (such as telegraph.co.uk) to commercial registrars. You pay an annual fee to "own" a domain name. ICANN then runs a system called DNS which maps these easily remembered domain names to the IP addresses where websites actually reside. Unless your users are willing to remember a long string of numbers such as 93.184.216.119, you have to buy into the domain name system.

Until Namecoin.

This crypto-currency is based on Bitcoin, but instead of acting like money it acts like internet addresses. It has claimed the .bit domain as its own and anybody with Namecoin can use it to reserve an address. And once you have it, it cannot be taken away: nobody can charge you an annual fee. Suddenly, a small part of ICANN's monopoly could disappear. For the first time, there is a viable alternative.

Now let's make a leap of imagination. It turns out that whole companies are also vulnerable to being replaced by Bitcoin offshoots. A project called Twister is attempting to replace Twitter with a peer-to-peer tool based on the blockchain, with messages instead of coins. Unlike Twitter, there is no central company to subpoena or coerce into handing out details of users. If you're an activist in the Middle East posting messages critical of the government, you may feel safer on Twister than Twitter.

Bitmessage aims to do the same thing for email. It's entirely safe, secure and anonymous, with no central point for storage for snooping agencies to target. Downloads of the program increased fivefold during June 2013 after news of email surveillance by the NSA emerged. Companies like Google, Yahoo! and Microsoft which offer webmail should be very worried indeed that there is a free, secure system on the horizon. And they are.

Not all of these replacement systems would be open-source and free. Some could run on the blockchain technology but still make people rich. Venture capitalist Fred Wilson, who spotted firms such as Twitter, Tumblr and Foursquare early, recently wrote in a blog post: "Our 2004 fund was built during social. Our 2008 fund was built during social and the emergence of mobile. Our 2012 fund was built during the mobile

downturn. And our 2014 fund will be built during the blockchain cycle. I am looking forward to it."

One lucrative area will be file storage. In the last few years we've become accustomed to keeping our files "in the cloud" rather than on our own machines. These services seem so simple: we upload our data and can then summon it at will from anywhere in the world. But they rely on huge data centres full of powerful servers, and multinational companies are the only ones with the resources to build them. Microsoft offer OneDrive, Apple has iCloud and there are others such as Dropbox. All offer a taste for free, but start charging once you pass a certain threshold. Now the Bitcoin protocol threatens this monopoly.

Atlanta-based Shawn Wilkinson is already famous in crypto-currency circles for creating Coingen, a simple service that builds clones of Bitcoin. Want to launch a new currency named after yourself? For just a few pounds Shawn can make it happen.

Now he's launching an online data storage service called Storj that will sit atop the Bitcoin network. Thanks to the thousands of miners, the currency is the largest computing network in the world, says Wilkinson. "Why just use that for money? We want to take the Bitcoin model and apply it to other systems."

The idea is that users' files would be hidden inside the blockchain (or pointers to that file, at least, otherwise the blockchain would quickly bloat to ludicrous proportions). An incentive program would reward those who offer up their own computers for the actual bulk of the storage. If you had a few gigabytes spare on your machine you could temporarily donate them to Storj and earn a few fractions of a Bitcoin each month.

This may sound horribly complex, but the user will be oblivious, says Wilkinson: "You don't care about the technical back-end. You just store your files and it works. When you use Dropbox you don't care about the technical part, you just care that it works." And people would switch in their droves, he claims, as the price would be orders of magnitude lower than the current offerings. "Were approaching a completely different economic model here. Now that we have these decentralised technologies, now that we've reduced the cost, what can we do with that? Bitcoin is the largest supercomputing network in the world – it outclasses the top 500 supercomputers by several orders of magnitude and has done since last year."

So what of Google, Apple or Amazon in the post-Storj world? Ultimately, physical computers and hard disks will still be needed. Files cannot be stored on clever ideas alone. But the huge companies that once cornered a market could be reduced to working for Storj in the hope of picking up incentive payments. No longer would there be rich pickings from users' monthly direct debits.

Braver, smarter companies could instead seize the opportunity to use the blockchain to their own end. Expensive business contracts and financial services could be cut out, for example. But why stop there?

Bitcoin is a decentralised network designed to replace the financial system. Ethereum is a decentralised network designed to replace absolutely anything that can be described in code: business contracts, the legal system or, as some of Ethereum's more evangelical backers believe, entire states.

Primavera De Filippi, a postdoctoral resreacher at CERSA/CNRS/Université Paris II, is one of Europe's most intellectually dazzling experts on digital and civil rights in cyberspace. She's currently at Harvard, exploring the legal challenges of decentralised digital architectures. Ethereum, she says, is "really sophisticated, and if any of these platforms are going to take off, I believe it's the one.

"It becomes a completely self-sufficient system, impossible to corrupt. It's a disruptive technology, and society will adapt to it, but it will be a slow process."

The other side of the law

So, what if we are on the verge of developing methods of data transformation that are impossible to corrupt? By definition, they will be impossible to police. And this is the point at which digital utopians begin to shift uneasily in their seminar chairs.

There's one bleedingly obvious venture where being safe from government matters more than anything else: drug dealing. The Silk Road catered for all illegal tastes

This is a touchy subject for many people working on legitimate Bitcoin startups, who feel that the Silk Road and other illegal sites have done irreparable reputational harm to the currency, associating it with cocaine, heroin and paedophiles, and therefore putting another hurdle in the way of mainstream adoption.

There has been an ongoing cat-and-mouse game between law enforcement and the founders of these sites. The Silk Road used Bitcoin for payments and hid behind the anonymising Tor network. But it was rumbled when the FBI tracked down the alleged founder and seized his servers. Because there was that

single point of failure, it all came crashing down.

But now developers have taken a leaf from the book of Bitcoin and are developing shopping websites which are themselves peer-to-peer. Amir Taaki is one of a group that recently walked away with the $20,000 first prize in a Toronto Bitcoin hackathon for a proof-of-concept demonstration called DarkMarket. Their idea was to create a fully decentralised shopping service, complete with transaction reviews, a safe escrow service to prevent fraud and user profiles. All of this hangs off Bitcoin's blockchain. There is no server for the FBI to seize, no owner to interrogate and no ISP to demand records from; it's the Hydra of online drug retail.

The developers claim that they won't be finishing it themselves – they're working on other Bitcoin projects. In any case, it would probably be wise not to announce your involvement in launching such a thing. But if it can be done, and demonstrably it can, it soon will be. A predictable weak link would remain. You still have to post drugs through the mail. This might not bring down the whole marketplace, but it could catch an individual seller if the FBI decide to buy a sample of heroin and use forensics to trace its origins. This is where the blockchain offers a futuristic solution – for sinister and legitimate retailers alike.

Mike Hearn, a former Google employee who left to work on Bitcoin, described in a recent lecture how the blockchain could be used to form bizarre new autonomous systems that would radically change our daily lives. He imagined iswarms of drones that could deliver small packages from A to B in an entirely secret and untraceable manner. This would present a huge opportunity for enterprising criminals, but also an enormous threat to the newly privatised Royal Mail and countless other courier companies.

Taxis in the cloud

Hearns described another scenario, set 50 years from now. A fictional character called Jen wants a taxi. She tells her smartphone where she's heading and it immediately starts gathering bids from nearby taxis and ranking them based on price and user reviews. This system on which requests and offers bounce around is called TradeNet, and it would be based on blockchain technology.

The strange thing about these vehicles is not that nobody drives them, as self-driving cars will have become commonplace decades before, but that nobody even owns them. They are what Hearn calls "autonomous agents", independent machines which earn their own money through fares, pays for their own fuel and repair and operates utterly without outside control.

All of this is made possible by Bitcoin. The B-word really is inescapable: it may be only one application of the blockchain but it has proved its power quite amazingly. Says Hearn: "If I go to a bank and try and open a bank account that is owned by a computer program, they'll tell me to get lost, or they'll think I'm crazy and report me to the police. But Bitcoin has no intermediaries, therefore there's really nothing to stop a computer just connecting to the internet and taking part all by itself. "All you need to instantiate a Bitcoin wallet is generate a large random number, and pretty much anything can do that. So these devices, they actually earn money and they pay their own costs. And this makes them the first form of artificial life truly worthy of the name."

These agents could turn to the TradeNet themselves in order to buy servicing, parts or even a whole new car, uploading their own software to it and therefore replicating. They could even hire human programmers to rewrite their code and upgrade them. Certainly, the very first agent would need to be created by humans. But what car company or taxi firm would choose to do such a thing, given the risk they pose to the bottom line? It would need to be done by the public in order to gain the benefits of ultra-cheap fares, probably following a Kickstarter-style funding model. Handily, that functionality is already built in to Bitcoin. "There is no such thing as a TradeNet today, but it is theoretically possible," says Hearn. "Which means that one day someone, somewhere will probably do it."

Liquid democracy

If you are looking to undermine centralised power, the biggest, most tempting target is government itself. There are lots of people trying to make inroads into the currency of democratic systems – dollars, sterling, euros, whatever – with the blockchain. Others want to replace state currencies entirely. Denmark has decided to take a very liberal policy with crypto-currencies, declaring that all trades will be tax-free; profits will be untouched, but losses will be non-deductible. It's no surprise, then, that this is one of the places it is being experimented with as an election tool.

The Liberal Alliance party, just seven years old, was founded on an ethos of economic liberalism – it

supports a flat rate income tax of 40 per cent, for example – and has begun to use technology built on Ethereum for internal votes. Party spokesman Mikkel Freltoft Krogsholm argued that it was an obvious choice for e-elections because it allows transparency and security and gives people the chance to "look under the hood" of the voting process. "From a liberal ideological point of view, it was an opportunity we just had to take," he said.

The blockchain makes perfect sense for this application because all transactions (they can be thought of as votes in this scenario) are recorded in perpetuity for reference. It also provides transparency so that a person can check that his or her vote was actually counted. Otherwise, how can you ever really be sure that your paper ballot made it to the final count?

Eduardo Robles Elvira is working on a similar but larger-scale system which he calls Agora Voting. It was developed as a tool for the Internet Party in Spain, which has a policy that all citizens should be able to vote on all matters in constant referenda. Rather than keep the code private he works with any party that wants to apply it to e-elections. It has already been successfully used in election primaries, with over 33,000 votes being cast.

The ultimate aim is "liquid democracy": not to just elect representatives and let them get on with it, and not necessarily to have direct referenda on each tiny issue, but to offer a system so flexible that a happy medium can be struck for every citizen. It can be best thought of as a social network designed not to help you share photographs, play games or communicate with your friends, but to run and manage your country. If you want to cast your vote on every issue, fine, that's possible. Or you can place your voting power in the hands of a career politician, as in the current system, or a knowledgeable friend or colleague.

And control could be infinitely fine: say you're a cyclist, you could hand over voting power on all road safety matters to a cycling charity that pushes for better infrastructure, but retain votes on economic matters and leave everything else in the hands of your local Liberal Democrat office.

"The idea behind liquid democracy is not to remove representative democracy with direct democracy, but to let you choose your means of democracy. You don't use an airplane to get to the street corner, and you don't walk from London to Tokyo: depending on what you want to do, you choose the means of transport," Robles told me. "We might see in the future a shift from trusting a single entity to trusting a computerised democratic and verifiable system, the same way that we saw a shift from trusting our healers and priests in the Middle Ages to trusting the scientific method. "It's just a glimpse into the future. It's like the first website: it doesn't have animations, it's not responsive, it may look now really basic, but still, it's the base of what we use now everyday, twenty years later. Maybe we will have a system more similar to ancient Athens, but scalable, where elected leaders are not so important."

It sounds appealing. But how does the blockchain record votes? In basic terms, with Agora, each voter gets some coins (in this case Zerocoins, an add-on to Bitcoin which shrouds transactions in anonymity) and they pay them into an account representing a choice. Imagine a yes/no referendum where the winning option is simply the account with the highest balance.

Again, as with all of these systems, this complex, mechanical stuff will be hidden from plain sight and the user will be presented with a simple-to-use interface, just as we don't need to know how our mobile phones, the internet or email truly works. Think of a nation state with an interface like Facebook: do you "like" this policy?

Blockchains versus banks

Andreas Antonopoulos is chief security officer at UK-based Blockchain.info, the world's largest Bitcoin wallet provider with over 1.1m registered users. Unlike many of the startups here, the company is several years old and already well respected in the Bitcoin community for building useful, reliable tools. Antonopoulos may be biased, in that case, but believes that the blockchain is one of the most important inventions of the 21st century. He sees it as a force for good, bringing bank accounts and access to international finance to the more than six billion people currently stuck in a cash-only economy. Many Africans have access to mobile phones and the internet, but not banking. It will also clean up and simplify the banking system.

"Most of the hierarchical institutions we have built around finance are there to regulate the fact that if you give a lot of money and put it under the control of a single person, history tells us that they tend to steal that money," says Antonopoulos. "That happens again and again. Almost all regulation is really to stop

one person with control over a lot of money from stealing that money. “This technology makes it largely unnecessary. The end result is that you’re going to see some pretty big changes. Those changes will be because there are now better ways of doing things, and people will choose those better ways. There’s nothing particularly libertarian about that. It’s simply a recognition that you can achieve in software what regulation has failed to achieve.”

Some of this will take the form of banks adopting blockchain technology themselves, replicating the services they offer now but with more transparency and lower overheads. It will also mean totally open services out of the control of any bank or organisation. Many services are obsolete – they just don’t know it yet.

“It’s ironic how what terrifies the banks today is actual free market capitalism. They don’t like that. They don’t like competition. Actually having to compete with smaller competitors that are more nimble and less costly is something that they’ve been able to prevent for years with the use of regulation as a barrier to entry.” This success in the financial sector will be a springboard to other industries and applications. And Antonopoulos shares the growing consensus that the blockchain will ultimately set its sights on democracy.

“People think Bitcoin is just a better way to do PayPal, and it’s not. Just like the internet, it’s a platform, and on that platform you can now build an incredible variety of things. “We can’t even imagine what things people are going to build. But just in the last year, from watching the startups in the space, I’ve been amazed at the range of innovation that occurs when you combine internet, the sharing economy and crypto-currencies. “This allows forms of self-organisation that don’t depend on parties or representative government at all. Representative democracy was a solution to a scaling problem. The fact that you couldn’t get a message across Europe in anything less than a couple of weeks.

“Well, that issue of scale has now been solved. So the question is, why do you need representatives? If you ask people who were born with the internet they can’t understand why we need them. To a whole generation of people [the phasing out of represnetative democracy] this is already a normal and natural progression. And now we have the tools to do that. “In my view, and this is probably why I call myself a ‘disruptarian’, centralised systems have one inevitable trajectory that has been validated throughout history, which is that as the people in the centre accumulate power and control they eventually corrupt the system entirely to serve their own needs, whether that’s a currency, a corporation, a nation. “Decentralised institutions are far more resilient to that: there is no centre, they do not afford opportunities for corruption. I think that’s a natural progression of humanity. It’s an idea that has existed for centuries and has progressively become more and more prevalent. The essential basics of going from monarchies to democracies, from distributing information, knowledge, education and wealth to the middle class, and power to simple people, has been a trend that has lasted now for millennia. This is not some kind of libertarian manifesto, or anarchist manifesto, saying that we don’t need mechanisms for achieving social cohesion. It’s simply recognising that we can create better mechanisms as we solve problems of scale. That’s all. It’s not some kind of crazy ‘we don’t need governments’ manifesto. It’s simply that we can make better governments when we don’t concentrate power as much in the hands of a few people. As my ancestors in Greece figured out more than three thousand years ago, power corrupts. You can read about that in the writings of the ancient greek philosophers, and nothing really has changed – only that scale of power, and the scale of misery that can be created when that power is wielded to do bad things.”

For all his optimism, Antonopoulos is proposing change so radical that it’s almost apocalyptic. Other digital utopians go even further. Daniel Larimer, who is working on a tool called Bitshares to apply blockchain technology to banking, insurance and company shareholding, believes that this new breed of technologies will ultimately render government entirely obsolete.

“I envisage a situation where governments aren’t necessary. That the free market will be able to provide all the goods and services to secure your life, liberty and property without having to rely on coercion. That’s where this all ultimately leads,” he told me. “The end result is that governments will have less power than free markets. Essentially, the free market will be able to provide justice more effectively and more efficiently than the government can. So, I see governments shrinking. If you think about it, what is the reason for government? It’s a way of reaching global consensus over the theory of right and wrong, global consensus over who’s guilty and who’s innocent, over who owns what. They’re going to be losing legitimacy as more open, transparent systems are able to provide that function without having to rely on force. That’s my mission in life.”

In his version of the future, identity and reputation will be the new currency. Laws and contracts will be

laid down in code and, if broken, reparations will be sought mathematically rather than through law enforcement agencies, courts and prisons. Those who cannot make good will be victim to "coordinated shunning" by the rest of the network – the whole of society. They will not be able to interact financially or in any other system running on the blockchain. They will be in an "economic prison". This will extend beyond being unable to make money transfers, because the blockchain will be in control of voting, commerce and communications. Being banished from this system would make life all but impossible.

"There are ways that you can structure society to achieve justice and encourage people to settle their debts," says Larimer. "There's a way to give small-town reputation on a global scale. It is ultimate libertarianism."

Or anarchy, depending on your point of view.

The blockchain is here to stay

What is clear is that the reactionary image of Bitcoin as a volatile, fragile currency for paedophiles and drug dealers is far off the mark. Just as the British pound, US dollar and euro, Bitcoin will be used for all manner of nefarious activities, but will also open up a world of opportunity.

As the first cryptocurrency, it may not last forever. But the blockchain technology which underpins it cannot be uninvented. It has already begun to worm its way into every aspect of our lives, swallowing up authority and distributing it to us via computer programs.

Programmers have already proved that these systems can be created. And logic follows that overheads and costs will be far lower than those of the commercial counterparts – the tottering giants of Facebook, Google, Amazon and so on. The big problem – and in the world of computers this has been solved so many times before – is that blockchain systems are complicated to use. But soon, they won't be. And then the masses will swarm towards them, creating a world we barely recognise.

HACKING ONLINE POLLS AND OTHER WAYS BRITISH SPIES SEEK TO CONTROL THE INTERNET

Glenn Greenwald; via Dave Barnby

http://www.911forum.org.uk/board/viewtopic.php?p=167590#167590
https://firstlook.org/theintercept/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-internet/

British Prime Minister David Cameron on Monday announced an investment of £1.1 billion (1.38 billion euros, $1.88 billion) into the armed forces, the bulk of it on intelligence and surveillance equipment. So what is he going to spend it on? Will it be more of:

JTRIG
(UNDERPASS)
(BADGER)
(WARPARTH)
(SILVERLORD)
(MINIATURE HERO)
(SPRING BISHOP)
(ANGRY PIRATE)
(SLIPSTREAM)
(GESTATOR)
(PREDATORS FACE)
(ROLLING THUNDER)
(ELATE)

(CHANGELING)
(IMPERIAL BARGE)

The secretive British spy agency GCHQ has developed covert tools to seed the internet with false information, including the ability to manipulate the results of online polls, artificially inflate pageview counts on web sites, "amplif[y]" sanctioned messages on YouTube, and censor video content judged to be "extremist." The capabilities, detailed in documents provided by NSA whistleblower Edward Snowden, even include an old standby for pre-adolescent prank callers everywhere: A way to connect two unsuspecting phone users together in a call.

The tools were created by GCHQ's Joint Threat Research Intelligence Group (JTRIG), and constitute some of the most startling methods of propaganda and internet deception contained within the Snowden archive. Previously disclosed documents have detailed JTRIG's use of "fake victim blog posts," "false flag operations," "honey traps" and psychological manipulation to target online activists, monitor visitors to WikiLeaks, and spy on YouTube and Facebook users.

But as the U.K. Parliament today debates a fast-tracked bill to provide the government with greater surveillance powers, one which Prime Minister David Cameron has justified as an "emergency" to "help keep us safe," a newly released top-secret GCHQ document called "JTRIG Tools and Techniques" provides a comprehensive, birds-eye view of just how underhanded and invasive this unit's operations are. The document is designed to notify other GCHQ units of JTRIG's "weaponised capability" when it comes to the dark internet arts, and serves as a sort of hacker's buffet for wreaking online havoc.

The "tools" have been assigned boastful code names. They include invasive methods for online surveillance, as well as some of the very techniques that the U.S. and U.K. have harshly prosecuted young online activists for employing, including "distributed denial of service" attacks and "call bombing." But they also describe previously unknown tactics for manipulating and distorting online political discourse and disseminating state propaganda, as well as the apparent ability to actively monitor Skype users in real-time--raising further questions about the extent of Microsoft's cooperation with spy agencies or potential vulnerabilities in its Skype's encryption. Here's a list of how JTRIG describes its capabilities:

* "Change outcome of online polls" (UNDERPASS)
* "Mass delivery of email messaging to support an Information Operations campaign" (BADGER) and "mass delivery of SMS messages to support an Information Operations campaign" (WARPARTH)
* "Disruption of video-based websites hosting extremist content through concerted target discovery and content removal." (SILVERLORD)
* "Active skype capability. Provision of real time call records (SkypeOut and SkypetoSkype) and bidirectional instant messaging. Also contact lists." (MINIATURE HERO)
* "Find private photographs of targets on Facebook" (SPRING BISHOP)
* "A tool that will permanently disable a target's account on their computer" (ANGRY PIRATE)
* "Ability to artificially increase traffic to a website" (GATEWAY) and "ability to inflate page views on websites" (SLIPSTREAM)
* "Amplification of a given message, normally video, on popular multimedia websites (Youtube)" (GESTATOR)
* "Targeted Denial Of Service against Web Servers" (PREDATORS FACE) and "Distributed denial of service using P2P. Built by ICTR, deployed by JTRIG" (ROLLING THUNDER)
* "A suite of tools for monitoring target use of the UK auction site eBay (www.ebay.co.uk)" (ELATE)
* "Ability to spoof any email address and send email under that identity" (CHANGELING)
* "For connecting two target phone together in a call" (IMPERIAL BARGE)

While some of the tactics are described as "in development," JTRIG touts "most" of them as "fully operational, tested and reliable." It adds: "We only advertise tools here that are either ready to fire or very close to being ready."

And JTRIG urges its GCHQ colleagues to think big when it comes to internet deception: "Don't treat this like a catalogue. If you don't see it here, it doesn't mean we can't build it."

The document appears in a massive Wikipedia-style archive used by GCHQ to internally discuss its surveillance and online deception activities. The page indicates that it was last modified in July 2012, and had been accessed almost 20,000 times.

GCHQ refused to provide any comment on the record beyond its standard boilerplate, in which it claims that it acts "in accordance with a strict legal and policy framework" and is subject to "rigorous oversight." But both claims are questionable.

British watchdog Privacy International has filed pending legal action against GCHQ over the agency's use of malware to spy on internet and mobile phone users. Several GCHQ memos published last fall by The Guardian revealed that the agency was eager to keep its activities secret not to protect national security, but because "our main concern is that references to agency practices (ie, the scale of interception and deletion) could lead to damaging public debate which might lead to legal challenges against the current regime." And an EU parliamentary inquiry earlier this year concluded that GCHQ activities were likely illegal.

As for oversight, serious questions have been raised about whether top national security officials even know what GCHQ is doing. Chris Huhne, a former cabinet minister and member of the national security council until 2012, insisted that ministers were in "utter ignorance" about even the largest GCHQ spying program, known as Tempora--not to mention "their extraordinary capability to hoover up and store personal emails, voice contact, social networking activity and even internet searches." In an October Guardian op-ed, Huhne wrote that "when it comes to the secret world of GCHQ and the [NSA], the depth of my 'privileged information' has been dwarfed by the information provided by Edward Snowden to The Guardian."

UEFI - THE MICROSOFT NSA KILL SWITCH

Judy Hope; BCG Bulletin

What is UEFI? According to Microsoft UEFI is:

UEFI (Unified Extensible Firmware Interface) is a standard firmware interface for PCs, designed to replace BIOS (basic input/output system). This standard was created by over 140 technology companies as part of the UEFI consortium, including Microsoft. It's designed to improve software inter-operability and address limitations of BIOS. Some advantages of UEFI firmware include:

Better security by helping to protect the pre-start-up – or pre-boot – process against boot-kit attacks.
Faster start-up times and resuming from hibernation.
Support for drives larger than 2.2 terabytes (TB).
Support for modern, 64-bit firmware device drivers that the system can use to address more than 17.2 billion gigabytes (GB) of memory during start-up.
Capability to use BIOS with UEFI hardware.

As we know, Microsoft and NSA teamed up a while back to gather our personal data with-out our consent. However, what is equally worrying is, Microsoft have now introduced a 'secure boot' system called UEFI on all their operating systems, since the arrival of Windows 8. The problem with that is three fold:

1. It locks-out the computer OWNER (you) from being able to install any other operating system on YOUR computer, other than Microsoft! Thus taking away your choice and making you a prisoner of Microsoft and endless anti-virus checkers! That part is bad news for those of us who prefer to use

GNU / Linux. Of course freedom is all about choice. Furthermore, the UEFI 'secure boot' system has nothing to do with keeping you or your computer secure, on the contrary it makes you more vulnerable in many ways!

2. With the new 'secure boot' system called UEFI, Microsoft can remotely access YOUR system and disable YOUR computer at any time! So not only do they have a back-door to your computer, but they now have the front door key as well! For built into the UEFI in what was 'the BIOS' (which instructs your computer which programs to run) they have embedded a code, that enables them to disable your Microsoft software! If and when they use it, your computer will not work until you purchase a new activation key from Microsoft and 'provided' they grant you one!

We all know they listen in on Skype, intercept our emails, but now they can now access our actual computer and its con-tent!

How many of you have used Microsoft's “Remote Assistance” in their support centre? Those of you who have will know their technical support team can; alter your email account settings on your computer, change printer driver or disable soft-ware 'they think' is a conflict, from the other side of world! If they don't like what they see on your hard drive, or in your browsing habits, they can switch your machine off. If they have the capacity to switch it off, then they can also switch it on without you knowing. Now that is very serious!

Who owns the machine you paid for, you or Microsoft? Who owns all the hard work you have put into articles and posts, you or Microsoft? Your own documents are YOUR intellectual property and you have a right to access and protect your own work, plus you have a right to privacy. But how could you access your own intellectual property if your software had been disabled by them? You couldn't and there lyeth the injustice, its not just a financial rip-off and a threat to us individually, but it has the potential to hamper national security by blocking or corrupting vital information.

3. Microsoft have even made all popular computer manufactures i.e. IBM, Dell, HP etc. sign a con-tract to support their new UEFI 'prison system'. Hence many firms have incorporated 'secure boot' hot keys, which resets the default start-up to Windows 8 even if you manage to disable the 'secure boot' . Thus Microsoft and most computer manufacturers are creating a monopoly to force out, any fare competition and choice for all consumers.

As for a solution, there is several things we can all do:

■ Boycott the well know computer manufactures who support the Microsoft UEFI system. Instead buy your next computer from someone 'reputable' who builds them and use any (free) Linux operating system, which is just as easy as MS, but far safer. The more people who boycott the well known brands of computers, the more profit those firms will loose out on. I can assure you, they will soon start thinking about who they should be loyal too.

■ Alternatively, if you buy a computer with Windows 7 on it, don't use the operating system, return it to Microsoft and ask for a re-fund! Tell them you that they have NO RIGHT to make you pay for their operating system which you have no intention of using! If more people do that they will soon get the message. Just remember the minuet you activate your Windows 8 (or whatever MS version it is) you are agreeing to their terms and conditions.

■ Or return the whole new computer and ask for a refund on grounds that it is “not fit for purpose”, for it will not allow you to load a different operating system and you refuse to be a prisoner of Microsoft. Ask the shop manager why are they favouring Microsoft's coercion over the customers freedom of choice.

■ Email Microsoft and tell them how you object to them taking away your choice and that you are not confident their system is safe to use, because of the growing number of viruses and all the data gathering which is done without your consent. So either they start making their software safer to use and protect our privacy (but they wont), or permit us to use another operating system which is safer. They cant have it both ways!

■ Email your MPs and ask what he or she plans to do to protect your online security, your personal work and freedom from Microsoft domination. After all, government in recent decades have made the internet almost compulsory, for various services that were once on our High Street now only operate online ….and that trend will only increase. However, we do have an 'off switch' if this abuse

of power continues.
■ Lastly we could do with some fully trained computer technicians who are willing to build computers and laptops with (free to use) Linux pre-installed. That would make the transition from Microsoft to Linux easier for anyone who chooses to break free from the Microsoft trap. Any volunteers? My point is; Microsoft is not the only operating system out there, nor is it the best or safest, all we need is the ability to choose for ourselves without Microsoft's coercive antics.

You may also like to read the following website
http://www.itproportal.com/2014/05/14/microsoft-openly-offered-cloud-data-fbi-and-nsa
Source / citation: http://freeyourselffrommicrosoftand-thensa.org/02-superbugs-and-cyber-wars/2-4-uefi-the-microsoft-nsa-kill-switch

WHY ARE TBTF BANKS SO HAPPY WITH THE EU BANKING UNION?

Don Quijones; Wolf Street; via Critical Thinking; freecriticalthinking.org.

On Tuesday, November 4th of this year, supervision of the Eurozone's 130 biggest banks, representing 80% of total financial assets, will be passed from national authorities into the welcoming hands of the ECB. From that day on, European banking union will be a reality.

The banks love the idea, as do apparently most Eurocrats, Members of the European Parliament, and national leaders. Even Angela Merkel and her government have finally come on board, in exchange for guarantees of quality surveillance, tighter coordination of economic policies, and more binding agreements."

As for the rest of the inhabitants of the Eurozone – all of whom will be impacted in one way or another – most are blissfully unaware that it is even happening. A new continent-wide banking system is taking shape right before our eyes and under our noses, but our eyes are closed and our noses are blocked. According to the official story, the citizens of Europe stand to benefit enormously from the banking union since it will impose greater control and tighter regulation of Europe's banks. It will also save taxpayers from having to fund future bailouts. The only problem is: if the main point of banking union is to protect taxpayers and bank customers, why do the continent's biggest banks seem so happy?

If the last six years have taught us anything, it is that when the big banks win, the rest of us lose. And if the banks lose (which, let's face it, rarely, if ever, happens these days) the one thing you can guarantee is that they and their powerful lobbying representatives will kick up the mother of all stinks. None of which is happening. Indeed, quite the contrary: rather than seeing the new system as a threat, the banks see it as an immense opportunity.

The Two "Cs": Consolidation and Concentration

Banking union will almost certainly intensify the concentration and consolidation of the banking sector. This, despite the fact that the European banking sector's most serious problem is the level of concentration – the mega banks that seem to be able to keep growing – and the fact that their sheer size and systemic importance make them impossible to resolve.

Thanks to a rather innocuous-sounding proposal called the "sales of business tool," big banks will soon be able to grow even bigger, by gobbling up smaller, weaker ones. To wit, from Corporate Europe Observatory:

Resolution authorities will explore if another big bank would be prepared to take over an ailing bank. The result will be even more concentration, and even bigger banks. This feature of the proposal is seen as a major opportunity by megabanks in Europe such as BNP Paribas.

When interviewed about the banking union, the CEO of BNP Paribas, Jean-Laurent Bonnafé, said: "Then the strongest part of the banking system could be part of some form of consolidation – either through an acquisition or through organic development plans."

The process would be led by the strongest banks in the most powerful economies, he said – and there would be an opportunity for BNP Paribas to benefit. "In the end, consolidation will just take out the weaker players who were unable to strengthen their positions either because of their own situation or because of their jurisdiction," he added.

No Glass-Steagall II

Banking union will not only exacerbate the too-big-to-fail syndrome and with it the scale of moral hazard on the continent, it will also do precious little to address the too-complex and too-interconnected-to-fail aspects of the banking system – two of the main causes of the ongoing global financial crisis.

In late 2008, when U.S. authorities began their autopsy on the Lehman Brothers' rotten corpse, they discovered that the bank was comprised of no less than 3,000 entities. Today's European megabanks are no different: Deutsche Bank, according to "anecdotal evidence" cited by FinanceWatch, is made up of about 2,000 entities.

As FinanceWatch has warned, "if the banks are not reformed such that they pose less of a systemic risk, they will simply block the mechanisms designed to resolve them."

This is exactly what appears to be happening. A perfect case in point is the Liikanen Report of 2012, which called for an end to the European tradition of universal banking and the adoption of an EU-wide Glass Steagall II. Even former Citigroup Chairman and CEO Sandy Weill, widely considered to be one of the driving forces behind the financial deregulation and "mega-mergers" of the 1990s, called for "splitting up" the commercial banks from the investment banks. "Bring back the Glass-Steagall Act of 1933 which led to half a century free of financial crises," he said.

Yet in Brussels no one seems to have listened. According to some experts, the proposal EU Single Market Commissioner Michel Barnier is preparing bears little resemblance to the Liikanen Group's proposal. It's also likely that the proposed firewalls will be riddled with loopholes.

There are many other deeply troubling features of the proposed model for banking union. They include watered-down capital and operational requirements; the ECB's potential conflict of interests in its new role as sole supervisor of the banking system (like the Fed, but with even more "independence" and power); and the continued emphasis on austere economic policies for the little people of Eurozone member states.

Of even greater concern is the chronic lack of funds to stabilize the system in the event of a repeat Lehman-type event.

Saving the System with Chump Change

The banking union has been sold to the public as a way of making the financial sector in general pay costs related to resolution. However, the "Single Resolution Fund" (SRF), which is supposed to be financed entirely by the banking sector itself (through a 1% tax on secured deposits in the Eurozone), will have at its disposal total funds of €55 billion.

Once upon a time €55 billion may have sounded like – indeed one day was – a lot of money. But in the world of modern-day banking, it's chump change. In fact, it would barely fill even a small crack in the €2-trillion balance sheet of France's biggest "too-big-to-fail" bank, BNP Paribas.

Just over a year ago FT columnist Walter Machau did some "back-of-the-envelope" calculations. He estimated that bad bank assets roughly constitute about 5% of Eurozone banking assets. If you throw in another 5% from hidden losses, the losses still being generated by the double-dip recession, and future losses through the bail-in of investors, you arrive at

around €2.6 trillion. So in effect, in Europe's new post-banking union reality, the SRF is somehow expected fill a one- or two-trillion-euro hole with just €55 billion of funds. Funds that apparently won't even be fully available until 2023.

Granted, in the event of a bank collapse, the ECB will also have the bail-in option to raise further capital. The bail-in clause is meant to ensure that bank shareholders and bondholders (and quite possibly depositors, too) pay a fair share of the costs of restitution. However, the maximum these investors would end up having to pay is 8% of the banks' liabilities, which is also unlikely to be enough to fill all the gaps.

As Bela Galgoczi, a Senior Researcher at the European Trade Union Institute (ETUI) in Brussels warns, this will leave only one option left for Brussels and Frankfurt – an option that just happens to be the exact same goal the senior architects of the European Project have been seeking all along. That's right, fiscal union:

Apart from a few enthusiasts, nobody would sign up for a "federal Europe" now, but step by step as an unintended consequence of a series of necessary decisions, we might end up there. The front door towards a "genuine monetary union" had not been accessible at the time of signing the Maastricht Treaty, debt mutualization was also not viable and as the latest example shows the monetization of Irish debt either.

As always, expediency remains the name of the Eurocrats' game. Their means are also the same: Obfuscation, opacity and lies. Especially when things "get serious". And right now, things could not be more serious. If banking union does get consummated – and by this point the only thing stopping it would be a financial bloodbath or political meltdown (hardly out of the question) – pretty much everything that is wrong with Europe's current financial system is almost certain to get worse. Not only that, but fiscal union would soon follow on its heels. And once Brussels has its own tax-raising powers, only one small step will remain in the old continent's mad stumble towards full-blown federalism: the holy grail of political union.

Don Quijones, freelance writer, translator in Barcelona, Spain. Raging Bull-Shit is his modest attempt to challenge the wishful thinking and scrub away the lathers of soft soap peddled by political and business leaders and their loyal mainstream media.
Negotiations behind closed doors are under way to water down all forms of financial regulation on both sides of the Atlantic via the Transatlantic Trade and Investment Treaty. Leading the charge: not the US government, but an unholy alliance between the European Commission, Wall Street, and the City of London. Read…. A Dark Alliance: European Union Joins Forces With Wall Street

PARASITE #1: THE SHADOW BANKING SYSTEM

Ellen Brown; Occupy.com; Web of Debt

One thing to be said for the women now heading the Federal Reserve and the IMF: compared to some of their predecessors, they are refreshingly honest. The Wall Street Journal reported on:

"Two of the world's most powerful women of finance sat down for a lengthy discussion Wednesday on the future of monetary policy in a post-crisis world: U.S. Federal Reserve Chairwoman Janet Yellen and International Monetary Fund Managing Director Christine Lagarde. Before a veritable who's-who in international economics packing the IMF's largest conference hall, the two covered all the hottest topics in debate among the world's central bankers, financiers and economists."

Among those hot topics was the runaway shadow banking system, defined by Investopedia as "the financial intermediaries involved in facilitating the creation of credit across the global financial system, but whose members are not subject to regulatory oversight. The shadow banking system also refers to unregulated activities by regulated institutions." Examples given include hedge funds,

derivatives and credit default swaps.

Conventional banks also engage in “shadow banking.” One way is by using their cash cushion as collateral in the repo market, where they can borrow to invest in the stock market and other speculative ventures. As explained by Bill Frezza in a January 2013 Huffington Post article titled “Too-Big-To-Fail Banks Gamble With Bernanke Bucks”:

"If you think [the cash cushion from excess deposits] makes the banks less vulnerable to shock, think again. Much of this balance sheet cash has been hypothecated in the repo market, laundered through the off-the-books shadow banking system. This allows the proprietary trading desks at these “banks” to use that cash as collateral to take out loans to gamble with. In a process called hyper-hypothecation this pledged collateral gets pyramided, creating a ticking time bomb ready to go kablooey when the next panic comes around."

Addressing the ticking time bomb of the shadow banking system, here is what two of the world’s most powerful women had to say:

"MS. LAGARDE: . . . You’ve beautifully demonstrated the efforts that have been undertaken . . . in terms of the universe that you have under your jurisdiction. But this universe . . . has generated the creation of parallel universes. And . . . with the toolbox with all the attributes that you have — what can you do about the shadow banking at large? . . .

"MS. YELLEN: So I think you’re pointing to something that is an enormous challenge. And we simply have to expect that when we draw regulatory boundaries and supervise intensely within them, that there is the prospect that activities will move outside those boundaries and we won’t be able to detect them. And if we can, we won’t be — we won’t have adequate regulatory tools. And that is going to be a huge challenge to which I don’t have a great answer."

Limited to her tools, there probably is no great answer. All the king’s horses and all the king’s men could not rein in the growth of the shadow banking system, despite the 828-page Dodd-Frank Act. Instead, the derivatives pyramid has continued to explode underits watch, to a notional value now estimated to be as high as $2 quadrillion.

At one time, manipulating interest rates was the Fed’s stock in trade for managing the money supply; but that tool too has lost its cutting edge. Rates are now at zero, as low as they can go – unless they go negative, meaning the bank charges the depositor interest rather than the reverse. That desperate idea is actually being discussed. Meanwhile, rates are unlikely to be raised any time soon. On July 23, Bloomberg reported that the Fed could keep rates at zero through 2015.

One reason rates are unlikely to be raised is that they would make the interest tab on the burgeoning federal debt something taxpayers could not support. According to the Treasury’s website, taxpayers pay about $400 billion a year in interest on the federal debt, just as they did in 2006 — although the debt has nearly doubled, from $9 trillion to over $16 trillion. The total interest is kept low by extremely low interest rates.

Worse, raising interest rates could implode the monster derivatives scheme. Michael Snyder observes that the biggest banks have written over $400 trillion in interest rate derivatives contracts, betting that interest rates will not shoot up. If they do, it will be the equivalent of an insurance company writing trillions of dollars in life insurance contracts and having all the insureds die at once. The banks would quickly become insolvent. And it will be our deposits that get confiscated to recapitalize them, under the new “bail in” scheme approved by Janet Yellen as one of the Fed’s more promising tools (called “resolution planning” in Fed-speak).

As Max Keiser observes, “You can’t taper a Ponzi scheme.” You can only turn off the tap and let it collapse, or watch the parasite consume its food source and perish of its own accord.

Collapse or Metamorphosis?

The question being hotly debated in the blogosphere is, “What then?” Will economies collapse globally? Will life as we know it be a thing of the past?

Not likely, argues John Michael Greer in a March 2014 article called “American Delusionalism, or Why History Matters.” If history is any indication, governments will simply, once again, change the rules.

In fact, the rules of money and banking have changed every 20 or 30 years for the past three centuries, in an ongoing trial-and-error experiment in evolving a financial system, and an ongoing battle over whose interests it will serve. To present that timeline in full will take another article, but in a nutshell we have gone from precious metal coins, to government-issued paper scrip, to privately-issued banknotes, to checkbook money, to gold-backed Federal Reserve Notes, to unbacked Federal Reserve Notes, to the “near money” created by the shadow banking system. Money has evolved from being “stored” in the form of a physical commodity, to paper representations of value, to computer bits storing information about credits and debits.

The rules have been changed before and can be changed again. Depressions, credit crises and financial collapse are not acts of God but are induced by mechanical flaws or corruption in the financial system. Credit may stop flowing, but the workers, materials and markets are still there. The system just needs a reboot.

Hopefully the next program that gets run will last more than 20 or 30 years. Ideally, we might mimic the ancient Mesopotamians, the oldest and most long-lasting civilization in history, and devise an economic system that lasts for millennia. How they did it, along with some other promising models, will be the subject of another article.

About Those Derivatives

How to kill the derivatives cancer without killing the patient? Without presuming to have more insight into that question than the head of the Fed or the IMF, I will just list some promising suggestions from a variety of experts in the field (explored in more depth in my earlier article):

Eliminate the superpriority granted to derivatives in the 2005 Bankruptcy Reform Act, the highly favorable protective legislation that has allowed the derivatives bubble to mushroom.
Restore the Glass-Steagall Act separating depository banking from investment banking.
Break up the giant derivatives banks.
Alternatively, nationalize the too-big-to-fail banks.
Make derivatives illegal and unwind them by netting them out, declaring them null and void.
Impose a financial transactions tax on Wall Street trading.
To protect the deposits of citizens and local governments, establish postal savings banks and state-owned banks on the model of the Bank of North Dakota, the only state to completely escape the 2008 banking crisis.

These alternatives are all viable possibilities. Our financial leaders, in conjunction with our political leaders, have continually re-created the web of money and credit that knits our economy together. But they have often taken only their own interests and those of the wealthiest citizens into account, not those of the general public. It is up to us to educate ourselves about money and banking, and to demand a system that is accountable to the people and serves our long-term interests.

Ellen Brown is an attorney, founder of the Public Banking Institute, and author of twelve books, including the best-selling "Web of Debt." In "The Public Bank Solution," her latest book, she explores successful public banking models historically and globally. Find Ellen Brown on the Commons

'If you want a vision of the future, think of a boot, stamping on a head, for ever - don't let it happen'.

George Orwell; thanks to Dave Barnby

POSTIVE MONEY BULLETIN

Ben Dyson; Postive Money Team

We've commissioned an exclusive poll of Members of Parliament to find out what they know about money. The results - which we'll be releasing very soon - are very worrying. If MPs don't understand that banks create 97% of the money in the economy, then they're blind to the dangers of another house price bubble or another debt-fuelled boom and bust.

So from now until the general election on 7th May 2015, we'll be campaigning to get MPs to understand why we need to democratise money. On 19th August, we will be asking you to email your MP with the results from the poll and check that your MP knows how money is created.

Volunteer to be a political coordinator

Alongside this we also want to find over 100 representatives for Positive Money to be our coordinators for contacting MPs up to the 2015 election.

Experience isn't necessary and you don't need to fully understand all the technical details - we will support you in the knowledge you need. All you need is enthusiasm to get involved and contact your MP. If this sounds like something you want to do please email Shirley at shirley@positivemoney.org

Look out for our email on 19th August!

Remember to email your MP on 19th August! It's crucial that we get MPs to understand how money is created so that we can start to build pressure for reform.

Upcoming Events

Hammersmith, August 27 ;Local Group Meetup
Walthamstow, September 5; Modernising Money reading group
London, September 17; DEBATE: Should economic growth be the primary goal of economic policy?
Lake District, September 19 – 21;Positive Money Retreat
Godalming, October 17; Quiz

From the Blog

Share prices with fractional reserve banking
El Mundo on Positive Money
Positive Money at The People's Parliament
Positive Money goes to the Lake District!

"Those who can make you believe absurdities can make you commit atrocities." -
Voltaire; thanks to Clive Menzies

RUNNYMEDE GAZETTE EDITED BY;- FRANK TAYLOR, 2 CHURCH VIEW, ST GILES TERRACE. CHETTON, BRIDGNORTH, SHROPSHIRE, WV16 6UG; Tel; (01746) 789326
frankinshropshire@hotmail.co.uk