RUNNYMEDE GAZETTE

A Journal of the Democratic Resistance

FEBRUARY 2014

CONTENTS

EDITORIAL

EDITORIAL

THE NECESSITY OF DEEP ROOTS

In the leading item Tony Cartalucci again hits the nail on the head. Any organisation, group or campaign can have all the wonderful analysis and ideas in the world, but if it has no means of communicating that message onto the doorsteps, and has no roots at that level, then all its work remains in vain.

We have yet to see whether events in Thailand actually result in the overthrow of the government. As in the Ukraine, surface events might be hiding deeper agendas. So-called 'colour revolutions' are not necessarily all they seem.

Sorting cause from pretext in the presence of several possible or actual conflicting parties, is often difficult and sometimes impossible. In any event, regimes and the deeper political cultures on which regimes rest frequently prove more durable than any particular set of faces in government. Cutting off the overgrowth is always a much easier task than digging up the roots.

But all that aside, at least the anti-government movement in Thailand seems to have drawn its energy from a wide social and political spectrum. Events in Ukraine are perhaps not so clear cut. The fog of rival propagandist narratives is now very dense indeed.

Resistance work in our own culture is mostly characterised by an unconnected series of small, exclusive, over-cerebral bubbles. Whilst communication, co-operation and co-ordination between these bubbles may have improved a little in recent times, it is still woefully short of adequate.

As happened across the Pond, Occupy, at least in its Mark I manifestation, must be considered to have been a failure in this country also. The question is whether there is going to be a Mark II.

At the moment the survivors of Occupy Mark I are engaged in what is essentially a series of policy forums focussing on such issues as TTIP, the health services, economic reform, citizens' income and so forth. Whilst such work is laudable, much of it is appears to be an attempt to re-invent the wheel, by going over ground already well researched elsewhere.

Meanwhile little, if any, thought seems to be given as to what the eventual aim of such work might be. Is this some form of nascent manifesto? If so, by what vehicle, and by what methods, might such a manifesto be brought to fruition? How are the 'pragmatic networks' of which Cartalucci speaks be brought into existence? How are a few dozen mostly rather cerebral individuals, based mainly in London and the Home Counties going to mobilise at least several hundred thousand people across the country?

DEFINING THE WEDGE

The problem is that whilst all this introspection, and policy fine tuning is going on, events may take a different turn. Do we want, in Cartalucci's words, a situation where, "*Today, individuals, or groups of individuals with no operational capacity are merely mobs in the streets - like barbarian raiders of ancient times - with no real plan, manifesto, or potential. They may be able to temporarily seize territory from their opponents but have absolutely no means to fortify it, let alone project power beyond it.*"?

Concentrating on micro-policy as akin to fiddling whilst Rome burns. In itself it can so easily become a form of diversionary activity which steers focus away from the mechanics by which such plans may be turned into reality. That is always something that can happen tomorrow. In the meantime, the priority is the search for that philosopher's stone of the perfect manifesto, supported by the unanswerable set of arguments.

What is needed in the immediate context is the macro-policy framework. What are the main driving principles? The detail can be adopted as events unfold. In any case, there is wide scope for experimentation especially in areas such as economic and monetary reform. In any case there will never be any definitive set of one-size-fits-all top down solutions.

Cartalucci talks of macro principles as 'wedge issues'. I might suggest that these are brief, simple, and definitive in drawing the line of demarcation between allies and opponents.

Keep it straight and keep it simple;-

1) Sovereignty. The ultimate power of control in all political and economic matters lies with the people. This principle sits at the apex of all others.

2) Subsidiarity. That no decision shall be taken at any higher level of governance that cannot be taken at the lowest possible level.

3) Justice. That all political and economic governance be conducted in accordance with the natural principles of justice, morality and equitability.

4) Currency. That no currency is to be created out of profit or for any other benefit than the Common Weal.

5) Democracy. That in accordance with the first principle, the people be able through referendum as of right and also through the power of the jury, to determine

the nature of their laws and government.

Within each of these parameters we can have many arguments about style and detail. But the time to get out there onto the doorsteps, and the time for all people of goodwill to join hands is long overdue.

That, for the moment, should be all that is needed.

“ *a free people have the right to determine government in their own image.”*
John Quincy Adams

Frank Taylor

WHY OCCUPY BANGKOK IS WORKING AND OCCUPY WALL STREET DIDN'T

Tony Cartalucci; Activist Post

Power flows from institutions and those without them have no power.

Occupy Wall Street, ideologically speaking, could not have been any more universally appealing. It was the 99% against the 1% (or more accurately - the 99.9% vs. the 0.1%), with the realization that big money had taken over politics and society to the detriment of all, regardless of political affiliation. With such a broadly appealing message, how come the movement fizzled?

Occupy Bangkok has exposed and hobbled the Wall Street-backed regime of Thaksin Shinawatra. It has succeeded where Occupy Wall Street hasn't because it is backed by numerous, influential institutions with wide and varied operational capacities. Tactically, economically, and politically, cornering, undermining or otherwise ending the protests have proved impossible for the regime.

Conversely, on the other side of the planet, "Occupy Bangkok" seeks to overthrow a regime propped up by Wall Street - that of billionaire despot Thaksin Shinawatra who for over a decade has served Western interests at great cost to the Southeast Asian nation of Thailand. Unlike Occupy Wall Street, Occupy Bangkok has been greatly successful. It has united unions, students, farmers, workers, business owners both big and small, against the corrosive influence of Thaksin Shinawatra and his Western backers.

Recent elections overseen by the regime unravelled in humiliation with less than half of the nation even choosing to vote. Of those that did, many defaced their ballots or checked "no vote" in protest. The protests which have been ongoing for months, have effectively hobbled the regime. Its collapse is now inevitable.

They have done so because they have institutions standing behind them, from media, to military, to courts, and large, influential political parties, as well as genuine, indigenous NGOs - all combining and coordinating against the regime and its foreign backers to equal or best every move they make.

The regime has been unable to move police against them in fear of provoking the military. They have been unable to financially cripple the protesters because of the large and diverse interests backing them through creative and ever shifting means. They have been unable to drown out the voice of the protesters because the protesters possess themselves large media platforms within Thailand, and alternative voices beyond, that are able to tell their side of the story.

None of this was present at Occupy Wall Street. The Western media was easily able to first turn it into a "left/right" wedge issue, then turn the "right" against the "left," before labelling the protesters as "fringe left," just before police swept protesters from the streets in swift, coordinated, and utterly unopposed operations across the country. The little political and institutional backing the movement did receive was merely superficial opportunism and theater to perpetuate America's false "left/right" political paradigm - some backing from establishment institutions like George Soros' Open Society, was designed in fact to undermine, not support the movement.

Institutions Make the World Go Round

Power stems from organized institutions. Empires were not built by mere armies and navies - they also included financial, economic, and institutional power projected beyond their borders into their colonies and subjects of conquest.

Today, individuals, or groups of individuals with no operational capacity are merely mobs in the streets - like barbarian raiders of ancient times - with no real plan, manifesto, or potential. They may be able to temporarily seize territory from their opponents but have absolutely no means to fortify it, let alone project power beyond it.

Imagine an Occupy Wall Street that before taking to the streets, had local and regional institutions organized for producing media, handling local infrastructure and social services, security, finance, and even organizing economic activity. When protesters took over parts of their cities, they could have turned them into microcosms of what they planned to do with the country once they succeeded in their overall goals of putting Wall Street back in its place. A well-organized movement able to expose the deficiencies of the ruling corporate-financier regime in America by example would have continuously expanded its success until it reached its goals.

A well organized movement with enumerated goals and operational capacity across a wide range of fields would also be very difficult to marginalize or undermine.

And although Occupy Wall Street was an overall failure, there was one bright point that illustrates that operational institutions are the foundation upon which a successful protest must be based - that bright point was "Occupy Sandy." Hurricane Sandy wrought destruction across New York City, and as expected, the local and federal government's response was one of apathy and incompetence.

The organizers of Occupy Wall Street turned their political machinery into pragmatic networks that filled in the gaps left by the poor government response. In a single stroke, the movement was able to make the point that not only was the government incompetent, but that their movement was fully capable of doing better without it.

The lesson to be learned is that instead of taking a political movement and turning it pragmatic in response to desperation in a crisis - activists must build pragmatic networks able to displace the corporate-financier elites' networks, and from this newly taken territory, project power through protests backed by functional, local and regional institutions of, by, and for the people.

Some examples that come to mind are unions, cooperatives, hackerspaces/makerspaces, community agriculture projects like Growing Power, alternative media networks, charity organizations, local educators, and even shooting clubs and volunteer emergency responders. All of these organizations may or may not see eye-to-eye politically, but pragmatically, they all seek to improve their local communities through hands-on pragmatic activism. While they may not be able to come together on wedge issues - the Occupy Wall Street movement with its universal appeal would have been a golden opportunity for them to come together and make an impact.

Thailand's Occupy Bangkok campaign proves that the real power of protests are to take territory from an unjust regime - but that territory must then be filled by the institutions backing the protests. If, like Occupy Wall Street, there are no such institutions, it is inevitable that the protests will eventually collapse. Occupy Wall Street, then, is not a failure, but a lesson to be learned from and built upon. The next time Americans take to the streets, hopefully they do so with their own indigenous institutions backing them.

Tony Cartalucci's articles have appeared on many alternative media websites, including his own at Land Destroyer Report, Alternative Thai News Network and LocalOrg.

BBC PROPAGANDA: “WHY I WANT A MICROCHIP IMPLANT”

Michael Snyder; Activist Post

Would you like to have an RFID microchip implanted under your skin? If you are anything like me, you would never allow such a thing to be done. But many others, especially among the younger generations, see things very differently. RFID microchip implants and other forms of “wearable technology” are increasingly being viewed as “cool”, “trendy” and “cutting edge” by young people that wish to “enhance” themselves. And of course the mainstream media is all in favour of these “technological advancements”.

For example, the BBC just published a piece entitled "Why I Want A Microchip Implant". We are told that such implants could solve a whole host of societal problems. Identity theft and credit card fraud would be nearly eliminated, many other forms of crime would be significantly reduced, children would never go missing and we wouldn't have to remember a vast array of passwords and PIN numbers like we do now. We are told that if we just adopted such technology that our lives would be so much better. But is that really the case?

As our society becomes "digitally integrated", technologists tell us that it is "inevitable" that wearable technology will become as common as smart phones are today. And the BBC article that I just mentioned is very eager for that day to arrive…

Ultimately, implanted microchips offer a way to make your physical body machine-readable. Currently, there is no single standard of communicating with the machines that underpin society – from building access panels to ATMs – but an endless diversity of identification systems: magnetic strips, passwords, PIN numbers, security questions, and dongles. All of these are attempts to bridge the divide between your digital and physical identity, and if you forget or lose them, you are suddenly cut off from your bank account, your gym, your ride home, your proof of ID, and more. An implanted chip, by contrast, could act as our universal identity token for navigating the machine-regulated world.

And for some people, that day is already here. In fact, at some technology conferences people actually line up to get chipped…

This month at the Transhuman Visions conference in San Francisco, Graafstra set up an "implantation station" offering attendees the chance to be chipped at $50 a time. Using a large needle designed for microchipping pets, Graafstra injected a glass-coated RFID tag the size of a rice grain into each volunteer. By the end of the day Graafstra had created 15 new cyborgs.

How creepy is that?

In addition, scientists have now developed batteries that are powered by the human body that could be used to provide a permanent power source for implantable technology. The following is a brief excerpt from a recent article by Kristan Harris entitled "Scientists Develop Human-Powered Battery For RFID Implantable Chips"…

A group of United States and Chinese researchers have collaborated to created a tiny implantable batteries that feed off of human energy. These thin, flexible mechanical energy harvesters have had been successfully tested on cows. The process uses what is known as conformal piezoelectric energy harvesting and storage from motions of the heart, lung, and diaphragm.

In the future, they say, it could be used to power a range of gadgets. Will it be long until you will charge your I-phone by plugging into your own body?

Of course RFID microchips don't actually have to be implanted to be useful. In fact, they are already being used to track schoolchildren all over the United States…

Upon arriving in the morning, according to the Associated Press, each student at the CCC-George Miller preschool will don a jersey with a stitched in RFID chip. As the kids go about the business of learning, sensors in the school will record their movements, collecting attendance for both classes and meals. Officials from the school have claimed they're only recording information they're required to provide while receiving federal funds for their Headstart program.

And over in the UK, RFID microchips are being used to track children wherever they go all day long…

For those who think the NSA the worst invader of privacy, I invite you to share an afternoon with Aiden and Foster, two 11-year-old boys, as they wrap up a Friday at school. Aiden invites his friend home to hang out and they text their parents, who agree to the plan.

As they ride on the bus Foster's phone and a sensor on a wristband alert the school and his parents of a deviation from his normal route. The school has been notified that he is heading to Aiden's house so the police are not called.

As they enter the house, the integrated home network recognizes Aiden and pings an advisory to his parents, both out at work, who receive the messages on phones and tablets.

We are rapidly entering a dystopian future in which it will be "normal" for technology to monitor our movements 24 hours a day. Most people will probably welcome this change, but it also opens up the door for an oppressive government to someday greatly abuse this technology.

Another type of "wearable technology" that is rapidly gaining acceptance is "smart tattoos".

Normally, we are accustomed to thinking of tattoos as body art. But that is about to change. Just check out this excerpt from a recent Gizmodo article…

Everyone from neurologists to biohackers is reinventing the very idea of the tattoo. With the right technology, tattoos can do a lot more than just look beautiful or badass. They can become digital devices as useful and complex as the smartphone that bounces around in your pocket. It sounds wildly futuristic, but the technology already exists.

In fact, a company called MC10 is working on a wide range of "smart tattoos" that will be able to do some pretty wild things…

Materials scientist John Rogers is doing some pretty incredible work with flexible electronics that stick to your skin like a temporary tattoo. These so-called "epidural electronics" can do anything from monitoring your body's vital signs to alerting you when you're starting to get a sunburn. Rogers and his company MC10 are currently trying to figure out ways to get the electronics to communicate with other devices like smartphones so that they can start building apps.

And Motorola actually has a patent for a tattoo that will take commands from unvocalized words in your throat…

The tattoo they have in mind is actually one that will be emblazoned over your vocal cords to intercept subtle voice commands — perhaps even subvocal commands, or even the fully internal whisperings that fail to pluck the vocal cords when not given full cerebral approval. One might even conclude that they are not just patenting device communications from a patch of smartskin, but communications from your soul.

They are calling it "wearable computing", and what we are witnessing now is just the tip of the iceberg.

What we will see in the future is probably far beyond anything that any of us could imagine right now. The following is from a recent Computer World article…

But imagine a future where anything you might want to know simply appears to you without any action or effort on your part. You could be eating in a restaurant, and Google Glass could, for example, tell you that it's the spot where your father proposed to your mother. Or that your friend will be late because of traffic, the salmon got bad reviews online, your parking meter will expire in 20 minutes, or the bathroom is through the bar and up the stairs to the right. Imagine that such knowledge could simply appear into your field of vision at the exact moment when you want to know it.

That's where wearable computing is going.

All of this may sound very "cool" to a lot of people. But what happens if we are all required to have "electronic identity tattoos" someday?

What happens if an oppressive government uses this technology to watch, track, monitor and control all of us 24 hours a day with this technology?

What happens if you are not able to get a job, have a bank account or buy anything without "proper identification"?

I think that you can see where I am going with this.

Technology is truly a double-edged sword. It can do great good, but it can also be used for great evil.

Michael T. Snyder is a former Washington D.C. attorney who now publishes The Truth. His new thriller entitled "The Beginning Of The End" is now available on Amazon.com.

HOW BIG BROTHER'S GOING TO PEEK INTO YOUR CONNECTED HOME

Nick Statt; Mobile World Congress

The tech industry easily convinced the public to accept a myriad of free services for the price of some loss of privacy. But getting them to embrace the smart home is going to be a far harder sell.

For as long as people have envisioned the inevitable advent of smart home, critics and privacy advocates have warned how it might all go horribly wrong.

We're not just talking Orwellian paranoia or a dystopian future where our personal lives are intertwined with corporate identities constantly siphoning data from them. The security and privacy issues at play in haphazardly wiring up our personal spaces are becoming increasingly more substantive and -- with the proliferation of smart devices -- opening up our lives to more points of vulnerability, both from real-world threats and existential ones.

"There's been nearly 600 million breaches of records since 2005. Those are the reported ones," said Will Pelgrin, the president and CEO of the Center for Internet Security. "It's almost a rite of passage of going through a data breach. I don't know anyone who hasn't been affected, whether it's email or the Target breach." And those numbers will only escalate as more data sources enter our lives -- and our homes. "The hackers out there trying to harvest this data are potentially in countries that don't prohibit it and they have a lot of time and some are well-funded," Pelgrin added.

The connected home vision has been around for decades. But until recently, futurists didn't worry much about privacy considerations because this Jetsons'-like scenario always seemed far over the horizon. All that changed last month when Google scooped up smart device-maker Nest Labs for $3.2 billion and pushed the privacy question off the back burner.

Fearing 'Big Brother' in the home

As the news hit the wire, the immediate reaction in some corners of the Internet was severe. Some swore never to purchase a Nest product now that Google owned the company. "There are some very good alternatives available which are not controlled, or have data collected from them, by Google," wrote one commenter here at CNET.

Others pointed to the recent revelations about the NSA's surveillance activities into the remotest corners of our lives. "We're inviting Google et al. to gain even more control over us? The world is going mad," wrote another. The Twitter snark and Google+ jokes came in torrents, and headlines like "Why is everyone disappointed by Google buying Nest?" aggregated the anger.

That wariness is now a common refrain when talking about Google as it expands aggressively into areas like robotics and ventures into personal health monitoring with far-out projects like glucose-measuring contact lenses. But putting aside the cheeky "Terminator" and HAL 9000 references, the second-guessing is more a testament to Google's ambition and seemingly limitless capabilities than it is a criticism of the company's privacy track record. No one has ever been substantially hoodwinked by Google with regards to their personal information. The way it handles data across its sprawling and free network of Web services, all of which funnel data into its ad infrastructure, is at this point well-known and more or less accepted by the people using its services.

Rather, people with legitimate concerns wove the Nest acquisition into a larger picture: a Google spin on the smart home could become overwhelmingly influential enough to careen the industry towards a model of free or cheap products with subtle data collection caveats we simply ignore out of apathy or because the alternatives aren't as good. In the age of NSA surveillance and mass adoption of data-sharing services and social networks, the threat of letting that strategy transition to the home is increasingly worrisome to those who think the option of keeping sacred certain aspects of our person lives should remain intact.

"The fact that when I'm sitting in front of my computer Google more or less knows what I'm doing, that doesn't seem to bother people too much," said Jean-Louis Gassée, a former Apple executive who regularly opines on tech trends in the industry blog Monday Note, wrote recently about the connected home and its many hurdles. "But if we broaden this to comings and going and in-house activities...for a lot of people, that's going to far."

And while Google has yet to make even one substantive move in the connected home beyond purchasing Nest -- that deal hasn't even closed yet -- it's become the face of the privacy discussion whether it wants to spearhead it or not. Nest CEO Tony Fadell and co-founder Matt Rogers have both been steadfast in their belief that transparency is key in retaining current and potential Nest customers' trust and that the company's terms of service should for now remain the same.

Still, Fadell's understandable yet telling refusal to say that Nest will never share data, and his admission at Germany's DLD Conference only one week after the acquisition announcement that a terms of service change would likely involve opt-ins, mean the privacy debate is only just getting started.

"I think we are pretty conscious, increasingly conscious, of how much Google knows about us in the digital world. With the ubiquity of sensors on our mobile phones, now they know where we are in the real world.," said Fatemeh Khatibloo, a Forester analyst who recently made the argument that Google's Nest acquisition will force a much-needed privacy debate about the Internet of things. "Now they're going to know exactly what we're doing in our home it starts to get a little bit scary. We're all very unsure as consumers what Google will and can do with that data."

The privacy play beyond Google and personal information

Foscam's digital video baby monitor is one of many "smart cameras" you can buy now. It was also discovered that it had severe vulnerabilities last summer, allowing a hacker to sprout profanity at and observe a Houston couple's 2-year-old child in her crib.

When it comes to the connected home, we're starting to see an abundance of choices: smart appliance lineups from Samsung and LG; cross-device communication software from Smart Things and Z-Wave; elegantly redesigned household staples like Nest's thermostat and smoke detector; and -- having arrived sooner and with more vulnerabilities than more recent smart home additions -- Internet-enabled cameras for home security and monitoring.

The home automation market is estimated to grow to more than $15 billion by the end of the decade, while the broader "Internet of things" market for connecting homes, businesses, and entire utilities and data industries is a "$19 trillion opportunity," Cisco CEO John Chambers boldly claimed at the Consumer Electronics Show last month.

That means going forward, the privacy discussion won't just revolve around what data is being shared, with whom and for what purposes as if the debate were the same conversation that privacy advocates have regarding Facebook. Instead, the connected home market -- with its many different products and platforms and no universal privacy protection -- is offering consumers a thousand different ways to "make the home smarter," with each coming with its own set of security risks and protection responsibilities that, if ignored or not followed carefully, can turn a system or product against its owner.

"My analogy is Fred Flintstone meets George Jetson," said Pelgrin. "Where Fred Flintstone is the users, we're getting this tech and we not only don't understand the benefits, but also the potential risks and challenges. There are some aspects of this that are tremendous."

Nowhere is that insight more apt than in the last decade's existing smart devices, consisting mostly of loosely protected home networks and IP cameras. Kashmir Hill, a Forbes reporter who last year detailed the vulnerabilities of such devices and networks by hacking into some herself, says that the threats are real, and thankfully at this time are only elementary. Similar to Hill's careful experiments, hackers would likely engage in activity like turning on and off lights or changing the television channel mostly for fun.

"I see that as a small-scale problem. I don't imagine massive attacks from China," she said. "But certainly thieves could figure out a way to manipulate technology." It could, and has in select instances already, venture into the creepy and sometimes criminal. Hill mentions specifically the instance last August in which a hacker tapped into a couple's Foscam baby monitor, spouting profanity at their 2-year-old and even discovering and then using the child's name by reading it off nursery wall using the monitor's camera.

In that vein, Hill sees Google's arrival in the space not as a reason to worry but as a source of relief if only in that it means we'll see more careful handling of privacy issues, a duty Google is more or less obligated to perform at this point to stave off criticism. "I tend to be more reassured when you have big companies that jump into this," Hill says. "The hacks that I've seen in the past are smaller companies. The infamous Foscam IP camera that was very easily hackable, TRENDNet IP cams, all over the net people were tapping into what they thought were private feeds."

In Hill's venturing into smart device vulnerabilities, she relied on one found within Insteon's home automation system that let an outdated product, one admittedly not originally designed for remote access, list a user's system through Google, where anyone could tap into it if the user failed to implement security measures that were voluntary, instead of required by default. Hill noted:

The dumb thing? Their systems had been made crawl-able by search engines -- meaning they show up in search results -- and due to Insteon not requiring user names and passwords by default in a now-discontinued product, I was able to click on the links, giving me the ability to turn these people's homes into haunted houses, energy-consumption nightmares, or even robbery targets. Opening a garage door could make a house ripe for actual physical intrusion.

That let Hill mess with people's lights -- something she did only after first contacting the unsuspecting users and asking to demonstrate the intrusion -- and in some cases even track down physical locations of the homes she was infiltrating if the user included street address information in the system name.

"As consumers we need to be cognizant to what we're agreeing to. How many of us really take the time to read the user license?" said Pelgrin. And it's that shift in responsibility, away from companies in an era when consumers expect to be wronged on the Web until the perpetrator backtracks its questionable practice, that marks an important shift with a connected home where the risks are higher and the data more sensitive.

With trade-offs & opt-ins, responsibility shifts to users

"I do think that are benefits of sharing data," said Alex Hawkinson, CEO of smart device- and software-maker Smart Things, in an interview CNET regarding the Nest acquisition earlier this month. "You can do a much better job at algorithms," he added of situations like brown outs, and aggregate that data for future use. "That of course can be all anonymized."

As Fadell expressed after the acquisition that opt-ins may play a large part in data sharing initiatives with the smart home down the line, the notion of a more transparent system -- one with incentives like a lowered energy bill -- that would let companies and consumers benefit symbiotically seems like a no-brainer. "Opt-ins in my opinion rate much better than opt-outs. As consumers we have the opportunity to help influence the marketplace and how data is used," Pelgrin noted.

"I really think that it's about transparency from a vendor perspective. It's about the customer understanding what they're signing up for. And do you want that to report back to the vendor? There's a good value in that, that they can improve that product or software," he added.

"I think it depends on how intimate the data is. I think a lot of people would say they wouldn't be bothered by the Nest data," said Hill. "But there was a big privacy debate about Kinect and Xbox [One] that was always on. That's more sensitive information."

Despite whatever kind of opt-ins arise, Hill is less worried about the idea of hacks or the specifics of added user responsibility than she is simply about the idea of having all our eggs in one basket. "More I just think about the fact that we'll be sending data all the time," Hill said, noting that a Google smart home platform may down the line be the best choice for consumers in that it will be the best designed and the most secure, but that that poses its own set of issues. "That's where you get into that paradox. You go with an established company that you're familiar with, but that means you're sharing more information with that company," she added.

No matter how it progresses, privacy in the connected home is about as complicated an issue as any the market will face in its long road to widespread adoption. Not only will companies like Google, Nest, Smart Things, and the numerous other players emerging seemingly every other week have to go to new heights with regards to transparency, incentivizing opt-ins, and thorny legal issues, but consumers can no longer aimlessly expect to use products and services until they get burned and move on. The lasting effects of a hack won't simply be a call to MasterCard or being asked to turn on two-factor authentication; intrusions both digital and potentially physical, unwarranted surveillance, and sensitive personal information leaking steadily to ad companies are all on the table.

And at the moment, that unfortunately means not taking companies or their products at face value while universal data protection and encryption and airtight security measures are in place. The burden is on us, and that's both good and bad, a teaching moment and also a sharing of power. "As people are more cognizant, I would hope that they would have more agency in deciding," Hill said. "And I hope the companies do stay ahead of the privacy and security because some of these services we'll be really nice and i hate to think we'll reject them."

"It's not new to the Internet of things. We've been giving up as consumers for a long time our finances, our identity -- a lot of the things about where we live and what we do already. Now our granular activity: when we watch TV, open the fridge, when you get in your car. It becomes that," Pelgrin said. "I think it is a time for all of us to take stock."

Nick Statt is a staff writer for CNET. He previously wrote for ReadWrite and was a news associate at the social magazine app Flipboard. He spends a questionable amount of his free time contemplating his relationship with video games while continuously exploring the convergence of tech, science and pop culture.

BIG BROTHER IS WATCHING YOU”. BEYOND ORWELL’S WORST NIGHTMARE

Marjorie Cohn; Global Research

Url of this article: http://www.globalresearch.ca/big-brother-is-watching-you-beyond-orwells-worst-nightmare/5367023

“Big Brother is Watching You,” George Orwell wrote in his disturbing book 1984. But, as Mikko Hypponen points out, Orwell “was an optimist.” Orwell never could have imagined that the National Security Agency (NSA) would amass metadata on billions of our phone calls and 200 million of our text messages every day. Orwell could not have foreseen that our government would read the content of our emails, file transfers, and live chats from the social media we use.

In his recent speech on NSA reforms, President Obama cited as precedent Paul Revere and the Sons of Liberty, who patrolled the streets at night, “reporting back any signs that the British were preparing raids against America’s early Patriots.” This was a weak effort to find historical support for the NSA spying program. After all, Paul Revere and his associates were patrolling the streets, not sorting through people’s private communications.

To get a more accurate historical perspective, Obama should have considered how our founding fathers reacted to searches conducted by the British before the revolution. The British used “general warrants,” which authorized blanket searches without any individualized suspicion or specificity of what the colonial authorities were seeking.

At the American Continental Congress in 1774, in a petition to King George III, Congress protested against the colonial officers’ unlimited power of search and seizure. The petition charged that power had been used “to break open and enter houses, without the authority of any civil magistrate founded on legal information.”

When the founders later put the Fourth Amendment’s prohibition on unreasonable searches and seizures into the Bill of Rights, they were attempting to ensure that our country would not become a police state.

Those who maintain that government surveillance is no threat to our liberty should consider the abuse that occurred nearly 200 years later, when FBI Director J. Edgar Hoover conducted the dreaded COINTELPRO (counter-intelligence program). It was designed to “disrupt, misdirect, discredit and otherwise neutralize” political and activist groups. During the McCarthy witch hunts of the 1950s, in an effort to eradicate the perceived threat of communism, our government engaged in widespread illegal surveillance to threaten and silence anyone with unorthodox political views. Thousands of people were jailed, blacklisted, and fired as the FBI engaged in “red-baiting.”

In the 1960’s, the FBI targeted Dr. Martin Luther King, Jr. in a program called “Racial Matters.” King’s campaign to register African-American voters in the South raised the hackles of the FBI, which disingenuously claimed that King’s organization was being infiltrated by communists. But the FBI was really worried that King’s civil rights campaign “represented a clear threat to the established order of the U.S.” The FBI went after King with a vengeance, wiretapping his phones, and securing personal information which it used to try to discredit him, hoping to drive him to divorce and suicide.

Obama would likely argue that our modern day "war on terror" is unlike COINTELPRO because it targets real, rather than imagined, threats. But, as Hypponen says, "It's not the war on terror." Indeed, the Privacy and Civil Liberties Oversight Board, an independent federal privacy watchdog, found "no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack."

The NSA spying program captures all of us, including European leaders, people in Mexico, Brazil, the United Nations, and the European Union Parliament, not just the terrorists. Although Obama assured us that the government "does not collect intelligence to suppress criticism or dissent," our history, particularly during COINTELPRO, tells us otherwise.

Obama proposed some reforms to the NSA program, but left in place the most egregious aspects. He said that the NSA must secure approval of a judge on the Foreign Intelligence Surveillance Court before it gets access to the phone records of an individual. But that is a secret court, whose judges are appointed by the conservative Chief Justice John Roberts, and it has almost never turned down an executive branch wiretapping request since it was created in 1978. Most significantly, Obama did not say that surveillance without judicial warrants or individual suspicion should be halted.

"One of [Obama's] biggest lapses," a New York Times editorial noted, "was his refusal to acknowledge that his entire speech, and all of the important changes he now advocates, would never have happened without the disclosures by [Edward] Snowden, who continues to live in exile and under the threat of decades in prison if he returns to this country."

Snowden's revelations will reportedly continue to emerge. And you can bet that Orwell will continue to turn in his grave for a long time to come.

Marjorie Cohn is a professor of law at Thomas Jefferson School of Law, a past president of the National Lawyers Guild, and deputy secretary general of the International Association of Democratic Lawyers. Her next book, Drones and Targeted Killing: Legal, Moral and Geopolitical Issues," will be published this fall by University of California Press.

BIG BROTHER WATCH

Nick Pickles; Big Brother Watch

GCHQ webcam snooping exposed (as were some of the users)

The latest revelation that GCHQ has been secretly intercepting and taking photographs from millions of people's webcam chats is as creepy as it gets. It is right that the security services can target people and tap their communications but they should not be doing it to millions of people. This is an indiscriminate and intimate intrusion on people's privacy.

It is becoming increasingly obvious how badly the law has failed to keep pace with technology and how urgently we need a comprehensive review of surveillance law and oversight structures. As more people buy technology with built-in cameras, from Xbox Kinect to laptops and smart TVs, we need to be sure that the law does not allow for them to be routinely accessed when there is no suspicion of any wrongdoing.

Our reaction featured on the front page of Metro as well as in the Daily Mail,Sky News, Independent and the Guardian.

Health database delay welcomed

In a campaign victory for Big Brother Watch, medconfidential and others, the care.data scheme has been delayed for six months. Following this, our Director gave evidence to the Health Select Committee on Tuesday.

The delay was the right thing to do. Patients have not been told enough about what is happening and the long term privacy implications of creating a new database and releasing data that could be used to re-identify patients. Key questions about safeguards and processes remain.

We will now work to address these concerns and ensure patient privacy is protected. You can download an opt-out form for care.data here.

Parliamentary event: Surveillance meets the internet

Big Brother Watch invites you to participate in the Internet society's event “Parliament meets Internet. Surveillance, the digital economy & the Open Internet.”

March 4th, from 5 to 7pm in Parliament - Committee room 12.

Scotland's state guardians

Last week the Scottish Government passed a staggeringly disproportionate piece of legislation that may see thousands of innocent families lives intruded upon by public sector busybodies.
unsubscribe from this list | update subscription preferences

Our submission to the ISC

Today campaign groups around the world are taking part in action to call for surveillance law reform. In Britain, we're making today by launching a new campaign - Don't Spy on Us - with a coalition of groups. We're proud to be joining forces with Liberty, Privacy International, the Open Rights Group, Article 19 and English PEN to fight mass surveillance.

Visit the dedicated campaign website, sign the petition and use it to contact your MP.

A key part of our work is ensuring that Parliament and relevant inquiries hear our arguments and policy analysis. The Intelligence and Security Committee of Parliament issued a call for papers on privacy and security and you can now read our submission.

Recent revelations have made clear the scale of intrusion on our privacy in the name of security, enabled by an explosion in digital communications and the computing resources available to the state.

President Obama’s NSA review panel recognised many of the issues involved in this arena and produced a thorough analysis of existing programmes, capabilities and concerns. This is a stark contrast to the convention of not discussing intelligence matters in the UK. This convention must be brought to an end, as it has now reached a farcical point where it prevents any meaningful debate in our outside of Parliament while also failing to provide any reassurance about legitimate surveillance activities.

Campaigning on medical privacy

As NHS England remains adamant to push through the care.data scheme despite concerns not being properly addressed, it was only a matter of time before GP’s started to publicly speak about. (Read our blog post here.)

A GP in Oxford has accused the NHS of using ‘blatantly bullying’ tactics to ‘bulldoze’ doctors and patients into complying with the scheme. The government has made several statements about the fact that GP’s are responsible for their patients’ data, yet it now appears that they are being told that they aren’t able to act when they have genuine concerns.

Big Brother Watch campaigning victories

As we have previously warned, the Lobbying Bill and the Anti-Social Behaviour Bill both posed threats to freedom of speech and civil liberties.

On both issues, we're pleased to report major successes. Of 100 amendments we supported to the Lobbying Bill, we succeeded in securing 98 of them. On the Anti-social behaviour Bill, the Home Office has now confirmed it will return to the existing legal threshold, requiring "harassment, alarm or distress" must be caused before a court can grant an injunction. The Government had proposed to allow injunctions for "conduct capable of causing nuisance or annoyance to any person".

We couldn't win these battles without your support and with other threats to our privacy and civil liberties on the horizon there are plenty of good reasons to support Big Brother Watch.

EU chief wants to block 'undesirable' websites

As we've previously warned, the UK's Anti-Extremism task force has already alluded to greater filtering of web content and now the EU has taken it one step further, with Gilles de Kerchove telling MPs he wanted to remove "not illegal, undesirable websites."

Setting out the action being taken by the EU he said: "The Commissioner for Home Affairs will set up a forum to discuss with the big players – Google, Facebook, Twitter – how we can improve the way one removes from the internet the illegal and if not illegal, undesirable websites."

Freedom of speech and of the press are essential parts of a free and democratic society. It should not be in the gift of politicians to decide what we read or who can write it and absolutely not on the basis of what some may consider undesirable. If content is to be blocked, it should be a decision taken by a court of law and only when a clear criminal test has been met establishing the content is illegal.

GCHQ legal challenge a priority for court

The European Court has completed its preliminary examination of our case and has communicated it to the British government, asking it to justify how GCHQ's practices and the current system of oversight comply with the right to privacy under Article 8 of the European Convention. The court has also given the case a rare priority designation. The government now has until 2 May to respond, after which the case will move into the final stages before judgment.

You can find out more on the website dedicated to the legal action PrivacyNotPrism.

follow on Twitter | like us on Facebook | forward to a friend | donate

Big Brother Watch in the media

Scandal of the children branded 'racist': Daily Express
More councils buy spy cars: Daily Mail
Fingerprint scanning in pubs attacked: Romford Recorder, Daily Star
NHS Database delayed: BBC, Health Sector, SC Magazine, Out-Law
Sunday Politics on surveillance : BBC
26 million images of cars logged every day by ANPR cameras: Guardian, Daily Mail, Telegraph
UK companies suffer from surveillance: City AM
PM justifies snooping on TV shows: Daily Mail, BBC
UK lags behind on privacy: Evening Standard, ITV, Guardian
The State of Surveillance: Total Politics
Opt-Out of Care.Data

Template letters are now available to send to your GP to inform them you do not wish to have your medical records included in the NHS' new care.data programme.

Harlan F. Stone, U.S. Chief Justice 1941-1946, on the Juror's Duty in the authentic Trial by Jury, as follows:

"If a juror feels that the statute involved in any criminal offence is unfair, or that it infringes upon the defendant's natural God-given unalienable or Constitutional rights, then it is his duty to affirm that the offending statute is really no law at all and that the violation of it is no crime at all, for no one is bound to obey an unjust law."

"That juror must vote Not Guilty regardless of the pressures or abuses that may be heaped on him by any or all members of the jury with whom he may in good conscience

disagree. He is voting on the justice of the law according to his own conscience and convictions and not someone else's. The law itself is on trial quite as much as the case which is to be decided."

U.S. Chief Justice Harlan F. Stone; Harvard Law Review.

Thanks to Kenn D'Oudney; Democracy Defined

500 YEARS OF HISTORY SHOWS THAT MASS SPYING IS ALWAYS AIMED AT CRUSHING DISSENT;

IT'S NEVER TO PROTECT US FROM BAD GUYS.

Washington's Blog; via Nathon Allonby

(A lengthy item, but well worth reading. It puts censorship and information control within Common Law jurisdictions into an historical context … including recent history. Effectively we and our privacy and anonymity are now living under a 'general warrant' … a device by the the assumption of innocence is vitiated and an entire population is considered to be guilty until proven innocent. Such an assumption underlies other bodies of legislation, for example so-called 'Vetting and Barring', and a raft of supposedly anti-fraud and money laundering regulations - Ed)

No matter which government conducts mass surveillance, they also do it to crush dissent, and then give a false rationale for why they're doing it.

For example, the U.S. Supreme Court noted in Stanford v. Texas (1965):

While the Fourth Amendment [of the U.S. Constitution] was most immediately the product of contemporary revulsion against a regime of writs of assistance, its roots go far deeper. Its adoption in the Constitution of this new Nation reflected the culmination in England a few years earlier of a struggle against oppression which had endured for centuries. The story of that struggle has been fully chronicled in the pages of this Court's reports, and it would be a needless exercise in pedantry to review again the detailed history of the use of general warrants as instruments of oppression from the time of the Tudors, through the Star Chamber, the Long Parliament, the Restoration, and beyond. What is significant to note is that this history is largely a history of conflict between the Crown and the press. It was in enforcing the laws licensing the publication of literature and, later, in prosecutions for seditious libel, that general warrants were systematically used in the sixteenth, seventeenth, and eighteenth centuries. In Tudor England, officers of the Crown were given roving commissions to search where they pleased in order to suppress and destroy the literature of dissent, both Catholic and Puritan. In later years, warrants were sometimes more specific in content, but they typically authorized of all persons connected of the premises of all persons connected with the publication of a particular libel, or the arrest and seizure of all the papers of a named person thought to be connected with a libel.

By "libel", the court is referring to a critique of the British government which the King or his ministers didn't like … they would label such criticism "libel" and then seize all of the author's papers.

The Supreme Court provided interesting historical details in the case of Marcus v. Search Warrant (1961):

The use by government of the power of search and seizure as an adjunct to a system for the suppression of objectionable publications … was a principal instrument for the enforcement of the Tudor licensing system. The Stationers' Company was incorporated in 1557 to help implement that system, and was empowered "to make search whenever it shall please them in any place, shop, house, chamber, or building or any printer, binder or bookseller whatever within our kingdom of England or the dominions of the same of or for any books or things printed, or to be printed, and to seize, take hold, *burn, or turn to the proper use of the aforesaid community, all and several those books and things which are or shall be printed contrary to the form of any statute, act, or proclamation, made or to be made. . . .*

An order of counsel confirmed and expanded the Company's power in 1566, and the Star Chamber reaffirmed it in 1586 by a decree

"That it shall be lawful for the wardens of the said Company for the time being or any two of the said Company thereto deputed by the said wardens, to make search in all workhouses, shops, warehouses of printers, booksellers, bookbinders, or where they shall have reasonable cause of suspicion, and all books [etc.] . . . contrary to . . . these present ordinances to stay and take to her Majesty's use. . . . "

Books thus seized were taken to Stationers' Hall where they were inspected by ecclesiastical officers, who decided whether they should be burnt. These powers were exercised under the Tudor censorship to suppress both Catholic and Puritan dissenting literature.

Each succeeding regime during turbulent Seventeenth Century England used the search and seizure power to suppress publications. James I commissioned the ecclesiastical judges comprising the Court of High Commission "to enquire and search for . . . all heretical, schismatical and seditious books, libels, and writings, and all other books, pamphlets and portraitures offensive to the state or set forth without sufficient and lawful authority in that behalf, . . . and the same books [etc.] and their printing presses themselves likewise to seize and so to order and dispose of them . . . as they may not after serve or be employed for any such unlawful use. . . ."

The Star Chamber decree of 1637, reenacting the requirement that all books be licensed, continued the broad powers of the Stationers' Company to enforce the licensing laws. During the political overturn of the 1640's, Parliament on several occasions asserted the necessity of a broad search and seizure power to control printing. Thus, an order of 1648 gave power to the searchers "to search in any house or place where there is just cause of suspicion that Presses are kept and employed in the printing of Scandalous and lying Pamphlets, . . . [and] to seize such scandalous and lying pamphlets as they find upon search. . . ."

The Restoration brought a new licensing act in 1662. Under its authority, "messengers of the press" operated under the secretaries of state, who issued executive warrants for the seizure of persons and papers. These warrants, while sometimes specific in content, often gave the most general discretionary authority. For example, a warrant to Roger L'Estrange, the Surveyor of the Press, empowered him to "seize all seditious books and libels and to apprehend the authors, contrivers, printers, publishers, and dispersers of them," and to "search any house, shop, printing room, chamber, warehouse, etc. for seditious, scandalous or unlicensed pictures, books, or papers, to bring away or deface the same, and the letter press, taking away all the copies. . . .]"

Although increasingly attacked, the licensing system was continued in effect for a time even after the Revolution of 1688, and executive warrants continued to issue for the search for and seizure of offending books. The Stationers' Company was also ordered "to make often and diligent searches in all such places you or any of you shall know or have any probable reason to suspect, and to seize all unlicensed, scandalous books and pamphlets. . . ."

And even when the device of prosecution for seditious libel replaced licensing as the principal governmental control of the press, it too was enforced with the aid of general warrants — authorizing either the arrest of all persons connected with the publication of a particular libel and the search of their premises or the seizure of all the papers of a named person alleged to be connected with the publication of a libel.

And see this.

General warrants were largely declared illegal in Britain in 1765. But the British continued to use general warrants in the American colonies. In fact, the Revolutionary War was largely launched to stop the use of general warrants in the colonies. King George gave various excuses of why general warrants were needed for the public good, of course … but such excuses were all hollow.

The New York Review of Books notes that the American government did not start to conduct mass surveillance against the American people until long after the Revolutionary War ended … but once started, the purpose was to crush dissent:

In the United States, political spying by the federal government began in the early part of the twentieth century, with the creation of the Bureau of Investigation in the Department of Justice on July 1, 1908. In more than one sense, the new agency was a descendant of the surveillance practices developed in France a century earlier, since it was initiated by US Attorney General Charles Joseph Bonaparte, a great nephew of Napoleon Bonaparte, who created it during a Congressional recess. Its establishment *was denounced by Congressman Walter Smith of Iowa, who argued that "No general system of spying upon and espionage of the people, such as has prevailed in Russia, in France under the Empire, and at one time in Ireland, should be allowed to grow up."*

Nonetheless, the new Bureau became deeply engaged in political surveillance during World War I when federal authorities sought to gather information on those opposing American entry into the war and those opposing the draft. As a result of this surveillance, many hundreds of people were prosecuted under the 1917 Espionage Act and the 1918 Sedition Act for the peaceful expression of opinion about the war and the draft.

But it was during the Vietnam War that political surveillance in the United States reached its peak. Under Presidents Lyndon Johnson and, to an even greater extent, Richard Nixon, there was a systematic effort by various agencies, including the United States Army, to gather information on those involved in anti-war protests. Millions of Americans took part in such protests and the federal government—as well as many state and local agencies—gathered enormous amounts of information on them. Here are just three of the numerous examples of political surveillance in that era:

In the 1960s in Rochester, New York, the local police department launched Operation SAFE (Scout Awareness for Emergency). It involved twenty thousand boy scouts living in the vicinity of Rochester. They got identification cards marked with their thumb prints. On the cards were the telephone numbers of the local police and the FBI. The scouts participating in the program were given a list of suspicious activities that they were to report.

In 1969, the FBI learned that one of the sponsors of an anti-war demonstration in Washington, DC, was a New York City-based organization, the Fifth Avenue Peace Parade Committee, that chartered buses to take protesters to the event. The FBI visited the bank where the organization maintained its account to get photocopies of the checks written to reserve places on the buses and, thereby, to identify participants in the demonstration. One of the other federal agencies given the information by the FBI was the Internal Revenue Service.

****

The National Security Agency was involved in the domestic political surveillance of that era as well. Decades before the Internet, under the direction of President Nixon, the NSA made arrangements with the major communications firms of the time such as RCA Global and Western Union to obtain copies of telegrams. When the matter came before the courts, the Nixon Administration argued that the president had inherent authority to protect the country against subversion. In a unanimous decision in 1972, however, the US Supreme Court rejected the claim that the president had the authority to disregard the requirement of the Fourth Amendment for a judicial warrant.

***

Much of the political surveillance of the 1960s and the 1970s and of the period going back to World War I consisted in efforts to identify organizations that were critical of government policies, or that were proponents of various causes the government didn't like, and to gather information on their adherents. It was not always clear how this information was used. As best it is possible to establish, the main use was to block some of those who were identified with certain causes from obtaining public employment or some kinds of private employment. Those who were victimized in this way rarely discovered the reason they had been excluded.

Efforts to protect civil liberties during that era eventually led to the destruction of many of these records, sometimes after those whose activities were monitored were given an opportunity to examine them. In many cases, this prevented surveillance records from being used to harm those who were spied on. Yet great vigilance by organizations such as the ACLU and the Center for Constitutional Rights, which brought a large number of court cases challenging political surveillance, was required to safeguard rights. The collection of data concerning the activities of US citizens did not take place for benign purposes.

***

Between 1956 and 1971, the FBI operated a program known as COINTELPRO, for Counter Intelligence Program. Its purpose was to interfere with the activities of the organizations and individuals who were its targets or, in the words of long-time FBI Director J. Edgar Hoover, to "expose, disrupt, misdirect, discredit or otherwise neutralize" them. The first target was the Communist Party of the United States, but subsequent targets ranged from the Reverend Martin Luther King, Jr. and his Southern Christian Leadership Conference to organizations espousing women's rights to right wing

organizations such as the National States Rights Party.
A well-known example of COINTELPRO was the FBI's planting in 1964 of false documents about William Albertson, a long-time Communist Party official, that persuaded the Communist Party that Albertson was an FBI informant. Amid major publicity, Albertson was expelled from the party, lost all his friends, and was fired from his job. Until his death in an automobile accident in 1972, he tried to prove that he was not a snitch, but the case was not resolved until 1989, when the FBI agreed to pay Albertson's widow $170,000 to settle her lawsuit against the government.
COINTELPRO was eventually halted by J. Edgar Hoover after activists broke into a small FBI office in Media, Pennsylvania, in 1971, and released stolen documents about the program to the press. The lesson of COINTELPRO is that any government agency that is able to gather information through political surveillance will be tempted to use that information. After a time, the passive accumulation of data may seem insufficient and it may be used aggressively. This may take place long after the information is initially collected and may involve officials who had nothing to do with the original decision to engage in surveillance.

Indeed, during the Vietnam war, the NSA spied on Senator Frank Church because of his criticism of the Vietnam War. The NSA also spied on Senator Howard Baker.
Senator Church – the head of a congressional committee investigating Cointelpro – warned in 1975:

[NSA's] capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide. [If a dictator ever took over, the N.S.A.] could enable it to impose total tyranny, and there would be no way to fight back.

This is, in fact, what's happened …
Initially, American constitutional law experts say that the NSA is doing exactly the same thing to the American people today which King George did to the Colonists … using "general warrant" type spying.
And it is clear that the government is using its massive spy programs in order to track those who question government policies.
Todd Gitlin – chair of the PhD program in communications at Columbia University, and a professor of journalism and sociology - notes:

Under the Freedom of Information Act, the Partnership for Civil Justice Fund (PCJF) has unearthed documents showing that, in 2011 and 2012, the Department of Homeland Security (DHS) and other federal agencies were busy surveilling and worrying about a good number of Occupy groups — during the very time that they were missing actual warnings about actual terrorist actions.
From its beginnings, the Occupy movement was of considerable interest to the DHS, the FBI, and other law enforcement and intelligence agencies, while true terrorists were slipping past the nets they cast in the wrong places. In the fall of 2011, the DHS specifically asked its regional affiliates to report on "Peaceful Activist Demonstrations, in addition to reporting on domestic terrorist acts and 'significant criminal activity.'"
Aware that Occupy was overwhelmingly peaceful, the federally funded Boston Regional Intelligence Center (BRIC), one of 77 coordination centers known generically as "fusion centers," was busy monitoring Occupy Boston daily. As the investigative journalist Michael Isikoff recently reported, they were not only tracking Occupy-related Facebook pages and websites but "writing reports on the movement's potential impact on 'commercial and financial sector assets.'"
It was in this period that the FBI received the second of two Russian police warnings about the extremist Islamist activities of Tamerlan Tsarnaev, the future Boston Marathon bomber. That city's police commissioner later testified that the federal authorities did not pass any information at all about the Tsarnaev brothers on to him, though there's no point in letting the Boston police off the hook either. The ACLU has uncovered documents showing that, during the same period, they were paying close attention to the internal workings of…Code Pink and Veterans for Peace.

***

In Alaska, Alabama, Florida, Mississippi, Tennessee, and Wisconsin, intelligence was not only pooled among public law enforcement agencies, but shared with private corporations — and vice versa. Nationally, in 2011, the FBI and DHS were, in the words of Mara Verheyden-Hilliard, executive director of the Partnership for Civil Justice Fund, "treating protests against the corporate and banking structure of America as potential criminal and terrorist activity." Last December using FOIA, PCJF obtained 112 *pages of documents (heavily redacted) revealing a good deal of evidence for what might otherwise seem like an outlandish charge: that federal authorities were, in Verheyden-Hilliard's words, "functioning as a de facto intelligence arm of Wall Street and Corporate America." Consider these examples from PCJF's summary of federal agencies working directly not only with local authorities but on behalf of the private sector:*

- *"As early as August 19, 2011, the FBI in New York was meeting with the New York Stock Exchange to discuss the Occupy Wall Street protests that wouldn't start for another month. By September, prior to the start of the OWS, the FBI was notifying businesses that they might be the focus of an OWS protest."*
- *"The FBI in Albany and the Syracuse Joint Terrorism Task Force disseminated information to… [22] campus police officials… A representative of the State University of New York at Oswego contacted the FBI for information on the OWS protests and reported to the FBI on the SUNY-Oswego Occupy encampment made up of students and professors."*
- *An entity called the Domestic Security Alliance Council (DSAC), "a strategic partnership between the FBI, the Department of Homeland Security, and the private sector," sent around information regarding Occupy protests at West Coast ports [on Nov. 2, 2011] to "raise awareness concerning this type of criminal activity." The DSAC report contained "a 'handling notice' that the information is 'meant for use primarily within the corporate security community. Such messages shall not be released in either written or oral form to the media, the general public or other personnel…' Naval Criminal Investigative Services (NCIS) reported to DSAC on the relationship between OWS and organized labor."*
- *DSAC gave tips to its corporate clients on "civil unrest," which it defined as running the gamut from "small, organized rallies to large-scale demonstrations and rioting."*
- *The FBI in Anchorage, Jacksonville, Tampa, Richmond, Memphis, Milwaukee, and Birmingham also gathered information and briefed local officials on wholly peaceful Occupy activities.*
- *In Jackson, Mississippi, FBI agents "attended a meeting with the Bank Security Group in Biloxi, MS with multiple private banks and the Biloxi Police Department, in which they discussed an announced protest for 'National Bad Bank Sit-In-Day' on December 7, 2011." Also in Jackson, "the Joint Terrorism Task Force issued a 'Counterterrorism Preparedness' alert" that, despite heavy redactions, notes the need to 'document…the Occupy Wall Street Movement.'"*

***

In 2010, the American Civil Liberties Union of Tennessee learned … that the Tennessee Fusion Center was "highlighting on its website map of 'Terrorism Events and Other Suspicious Activity' a recent ACLU-TN letter to school superintendents. The letter encourages schools to be supportive of all religious beliefs during the holiday season."

***

Consider an "intelligence report" from the North Central Texas fusion center, which in a 2009 "Prevention Awareness Bulletin" described, in the ACLU's words, "a purported conspiracy between Muslim civil rights organizations, lobbying groups, the anti-war movement, a former U.S. Congresswoman, the U.S. Treasury Department, and hip hop bands to spread tolerance in the United States, which would 'provide an environment for terrorist organizations to flourish.'"

***

And those Virginia and Texas fusion centers were hardly alone in expanding the definition of "terrorist" to fit just about anyone who might oppose government policies. According to a 2010 report in the Los Angeles Times, the Justice Department Inspector General found that "FBI agents improperly opened investigations into Greenpeace and several other domestic advocacy groups after the Sept. 11 terrorist attacks in 2001, and put the names of some of their members on terrorist watch lists based on evidence that turned out to be 'factually weak.'" The Inspector General called "troubling" what the Los Angeles Times described as "singling out some of the domestic groups for investigations that lasted up to five years, and were extended 'without adequate basis.'

Subsequently, the FBI continued to maintain investigative files on groups like Greenpeace, the Catholic Worker, and the Thomas Merton Center in Pittsburgh, cases where (in the politely put words of the Inspector General's report) "there was little indication of any possible federal crimes… In some cases, the FBI classified some investigations relating to nonviolent civil disobedience under its 'acts of *terrorism' classification."*

***

In Pittsburgh, on the day after Thanksgiving 2002 ("a slow work day" in the Justice Department Inspector General's estimation), a rookie FBI agent was outfitted with a camera, sent to an antiwar rally, and told to look for terrorism suspects. The "possibility that any useful information would result from this make-work assignment was remote," the report added drily. "The agent was unable to identify any terrorism subjects at the event, but he photographed a woman in order to have something to show his supervisor. He told us he had spoken to a woman leafletter at the rally who appeared to be of Middle Eastern descent, and that she was probably the person he photographed."

The sequel was not quite so droll. The Inspector General found that FBI officials, including their chief lawyer in Pittsburgh, manufactured postdated "routing slips" and the rest of a phony paper trail to justify this surveillance retroactively.

Moreover, at least one fusion center has involved military intelligence in civilian law enforcement. In 2009, a military operative from Fort Lewis, Washington, worked undercover collecting information on peace groups in the Northwest. In fact, he helped run the Port Militarization Resistance group's Listserv. Once uncovered, he told activists there were others doing similar work in the Army. How much the military spies on American citizens is unknown and, at the moment at least, unknowable.

Do we hear an echo from the abyss of the counterintelligence programs of the 1960s and 1970s, when FBI memos — I have some in my own heavily redacted files obtained through an FOIA request — were routinely copied to military intelligence units? Then, too, military intelligence operatives spied on activists who violated no laws, were not suspected of violating laws, and had they violated laws, would not have been under military jurisdiction in any case. During those years, more than 1,500 Army intelligence agents in plain clothes were spying, undercover, on domestic political groups (according to Military Surveillance of Civilian Politics, 1967-70, an unpublished dissertation by former Army intelligence captain Christopher H. Pyle). They posed as students, sometimes growing long hair and beards for the purpose, or as reporters and camera crews. They recorded speeches and conversations on concealed tape recorders. The Army lied about their purposes, claiming they were interested solely in "civil disturbance planning."

Yes, we hear echoes to the Cointelpro program of the 60s and 70s … as well as King George's General Warrants to the Colonies … and the Star Chamber of 15th century England.

Because – whatever governments may say – mass surveillance is always used to crush dissent.

Notes:

1. Spying is also aimed at keeping politicians in check.
2. The East German Stasi obviously used mass surveillance to crush dissent and keep it's officials in check … and falsely claimed that spying was necessary to protect people against vague threats. But poking holes in the excuses of a communist tyranny is too easy. The focus of this essay is to show that the British and American governments have used this same cynical ruse for over 500 years.
3. For ease of reading, we deleted the footnotes from the two Supreme Court opinions.

2,000 NHS PATIENTS' RECORDS ARE LOST EVERY DAY WITH MORE THAN TWO MILLION SERIOUS DATA BREACHES LOGGED SINCE THE START OF 2011

Sophie Borland; Daily Mail

Records have been mistakenly sold on eBay or dropped in the street
Staff are also sending sensitive information to the wrong places
One NHS Trust said information had been thrown into bins

Fears they will fall into private hands - who will use them to make a profit

Lost Medical records have been dumped in landfill sites, dropped in the street and even left in grocery stores. Lost: Medical records have been dumped in landfill sites, dropped in the street and even left in grocery stores.

The NHS is losing the files of almost 2,000 patients every day. More than two million serious data breaches have been logged since the start of 2011, official figures show.

Medical records have been mistakenly sold on eBay, dumped in landfill sites, dropped in the street and even left in grocery stores. Staff are also sending sensitive information to the wrong places or publishing it on websites.

The figures are especially worrying because next month the NHS starts harvesting personal data from confidential medical files. It will be stored on a national computer database and used to analyse trends and improve care.

There are fears however the data will fall into the hands of private firms – including insurers – who will use it to make a profit.

A poll yesterday showed only 29 per cent of adults recall receiving a leaflet explaining the NHS England scheme. The ICM Research survey for the BBC suggests many patients will not know they can block the use of their data.

A growing number of family doctors oppose the scheme and earlier this week the Royal College of GPs called for the project to be halted. It warned of a ‘crisis in public confidence’.

The scale of the losses of medical records emerged in figures obtained from the Office of the Information Commissioner.

The 2,152,560 lapses are almost certainly an underestimate because NHS staff are obliged to report only serious losses.

In one extraordinary blunder, NHS Surrey admitted that three computers containing personal information on 3,000 adults and children had been sold on eBay. The trust – abolished last year – had passed on the computers to be recycled unaware that the files were still stored on them.

Mislaid: Some files were even, mistakenly, sold on eBay

A South London healthcare trust reported that in 2012 a staff member had left a clipboard containing personal information about patients in a grocery store. University Hospitals Coventry and Warwick admitted medical files had been dumped in the bin on two separate occasions. The records were retrieved by members of the public. In most lapses it is thought that NHS staff simply failed to keep records confidential – either by mislaying copies or sending them to the wrong address.

Roger Goss, of the campaign group Patient Concern, said: ‘The NHS has an appalling record and barely a month goes by without you hearing of staff losing laptops or mislaying memory sticks. But the reason the medical profession – and ourselves – are so opposed to the [data harvesting] scheme is that patients will not want to share private information about themselves with their GP for fear of it being sold or ending up online. This will lead to their diagnosis and treatment being delayed and the standard of care will deteriorate.’

At least four GPs are so opposed to the scheme they have opted out all of the thousands of patients on their lists – apart from a handful who want to take part. One, Gordon Gancz, who is based in Oxford, was warned by NHS England that such actions could cost him his job.

Professor Brian Jarman, an expert in hospital data, warned insurers might be able to track down patients if they were given access to the national database. He said: ‘The GP data is considerably more extensive than the hospital data because there are many more episodes of care. Although it would be illegal, I think it would be possible for a skilled researcher to link a few cases with personal information held by an insurance company. The data is potentially useful but we must be very careful with its use, fully inform the public and get their cooperation. I would therefore prefer the data extract planned for March be postponed so that we can get it right.’

NHS England insists the records will be anonymous – using dates of birth and addresses instead of names.

Read more: http://www.dailymail.co.uk/news/article-2559876/2-000-NHS-patients-records-lost-day-two-million-data-breaches-logged-start-2011.html#ixzz2uQiSit

NANOBIOMETRICS WILL TRACK YOU BY SMELL

Nicholas West; Activist Post

In a few short years, we already have become accustomed to drone surveillance and an array of biometric ID tracking technology that has formed a pervasive matrix of identification and personal data retention.

As discussed in How Close Are We to a Nano-Based Surveillance State? back in February of 2011, the next phase of ID will be on the nano scale. DARPA and their contractors have been working for quite a while on making you, not just your personal data, the tracking mechanism. Through a matrix of biological sensors and biometrics, the individual is now set to be tracked, traced and databased with greater frequency and much greater ease.

A new announcement from a Spanish engineering firm highlights the direction that is being taken in extracting the most innate personally identifying information possible. We already have iris scans, biometric fingerprinting, facial recognition, voice recognition, payment with vein scans, and proposals for brain scan databases. Now our unique smell is being researched as the ultimate tool for providing one's ID authentication.

Nanotechnology for identification purposes already has been introduced in the following ways, just to name a few:

Nano sensors for use in agriculture that measure crops and environmental conditions.
Bomb-sniffing plants using rewired DNA to detect explosives and biological agents.
"Smart Dust" motes that wirelessly transmit data on temperature, light, and movement (this can also be used in currency to track cash).
Nano-based RFID barcodes that can be embedded into any material for tracking of all products . . . and people.
Nanosensors that can detect molecular changes indicating the presence of diseases.
Devices to detect molecules, enzymes, proteins and genetic markers -- opening up the door for race-specific bioweapons, as mentioned in the Project For a New American Century's policy paper Rebuilding America's Defenses.

It is these last points that makes using ones genetic markers particularly troubling. For example, it already has been proposed to employ genetic pat-downs for use in airport screening. And, in fact, the company researching the concept of nanoscale smell sensor ID - Ilía Systems Ltd - highlights security applications such as airport screening and national border control.

Quick to assuage concern over Big Brother, however, a press release from Universidad Politécnica de Madrid sees this technology merely as an extension of what already has been used from the beginning - just think of it as an electronic bloodhound:

People body odour identification is not a new idea considering since it has been conducting for over a century by the police force thanks to the help of bloodhounds dogs which are trained for such task. The ability of these dogs to follow the trail of a person from a sample of his or hers personal odour is well known and proofs that using body odour is effective is an effective biometric identifier. Although the sensors used today have not yet achieved the accuracy dog's sense of smell, the research has used a system developed by the Ilía Sistemas SL company that has a high sensitivity to detect volatile elements present in body odour.

The difference, I would argue, is that the traditional bloodhound itself doesn't have the ability to transmit information instantaneously to an array of databases to be analysed, stored, and used for future tracking applications by government agencies or private interests.

We only need to look at the applications that have been admitted to in order to realize that this type of technology is far vaster in scale than authenticating our ID for our own personal financial security, or for disease detection and prevention.

By 2003, the newly opened Department of Homeland Security showed immediate interest in SensorNet, a program spearheaded by Oak Ridge National Laboratory and their strategic partners to research ways to fully integrate nano- and micro-sensors into one overall Internet-like matrix of real-time detection and surveillance. The Department of Defense allocated $3 million to the initiative for the first year, with a projected budget into the billions being allocated over the long term for "detection systems."

By 2006, Oak Ridge announced that they planned to turn Fort Bragg military base into a prototype for America's future cities. According to Department of Energy researcher, Bryan Gorman, "Any sensor can talk to any application. Just like with the Internet or with telephone systems, it doesn't matter what kind of computer or telephone you have, where you are or what application you're running. The system just works."

SensorNet has since morphed into an even more comprehensive system "to integrate safety and security measures . . . into the transportation system," which includes concerns surrounding transportation and commerce in the "political, economic, or environmental" arenas.

What we are really seeing with this development of smell ID is what we typically see with creeping surveillance technology: first it is introduced through the potential benefits in the area of disease detection and protection from terrorism, real and financial - all voluntary, of course - before it becomes a pervasive and permanent (and mandatory) part of the human landscape. The potential for abusing this type of technology by integrating it across currently disparate lines is virtually certain in our currently data-compromised world.

Legitimate science must research ways to increase human potential and freedom, not permit it to be used as a system for identification and control by the politically and morally compromised. With the rise of nanotechnology as a federal initiative, we should strongly resist the collection of any part of our life force to be used in whichever ways that government-controlled science sees fit.

It is the misappropriation of science and technology that poses one of the greatest threats to our freedom. How much longer can we permit the ethical part of this discussion to become an afterthought, instead of an integral component while beginning this type of research?

Recently by Nicholas West:

Economic Elite Announce Plan to Replace Human Labor with Machines
All In The (Robotic) Family: New Study Aims to Develop Emotional Bond Between Humans and Androids
Medical Nanobots Will Connect Brain to Cloud Computing - Ray Kurzweil

MEDIA CENSORSHIP THAT DARE NOT SPEAK ITS NAME: WHAT IS RADICAL INTELLECTUAL ACTIVITY?

James F. Tracy; Global Research

This is a revised set of remarks given at “The Point is to Change It” conference on November 1, 2013 at the University of San Francisco. The event was co-sponsored by Project Censored.

The panel on which I participated was organized by Project Censored Director Mickey Huff to address the contrast between the radical journalistic activity practised by Project Censored and the decade-old US media reform movement that has sought to initiate broader policy changes at the federal level. In previous years PC has been excluded from media reform events, likely because of its research and criticism of foundation-funded progressive-left media and the censorial practices they impose on themselves and their peers.

The feedback from conference-goers to the panel’s observations was predictable. For example, “9/11 Truth has no facts. Look at how it relies on Alex Jones and Loose Change. Let’s move on.” [Read: I shall not be identified with amateurs and fanatics. Or, Why risk being perceived as politically incorrect.] And, “It is impossible to be radical without a vigorous critique of capitalism.” [Read: Extreme historical myopia is sometimes practical and necessary. Or, 9/11 is a career-ender.]

I appreciate Project Censored’s invitation to participate in the event and its continued endeavours to spread the word on the fundamental relationship between mass media and the broader political economy.

What does it mean to be radical? What is radical intellectual activity? It involves identifying, examining, and publicizing the root causes of major problems in the body politic that hinder the full realization of each individual’s human capacities.

What are the possible areas where such inquiry may take shape? The “News Clusters” that

Project Censored has been using in its recent yearbooks provide a rough outline: the economy, war, health and the environment, the viability of the commons (as evidenced by Iceland), and civil liberties and freedom of expression, because without the ability to be able to express ourselves we cannot demonstrate our freedom and contest wrongdoing.

Around the time I was born Noam Chomsky wrote "The Responsibility of Intellectuals," suggesting that radical intellectual activity along these lines is necessary if we are to survive as a species. "It is the responsibility of intellectuals to speak truth and expose lies," Chomsky asserted.[1]

Aside from Chomsky's abandonment of this principal in terms of questioning deep events, the mid-to-late 1960s was a far different world from the one we inhabit today. In contrast to the 1960s, there is now a fast-emerging police state, the loss of Constitutional protections, a "war on terror" we are told will be without end, and huge economic disparities. And so any such responsibility is much greater than it was then because the stakes are much higher.

Scholars with institutional backing have some security from which to operate along these lines. Apart from the support afforded through an academic position, the greatest hindrance to carrying out radical intellectual activity involves the question of money and resources.

With this in mind there is a tendency for progressive-left media to inordinately rely on funding from tax-free foundations, with attendant consequences for their output. This is no better illustrated than in John Pilger's first-hand account in Project Censored's most recent volume.

In 2011 Pilger's The War You Don't See became "the film you don't see" courtesy of the Lannan Foundation pulling the rug out from underneath Pilger as he was about to embark on a US tour promoting the work.

What is at least as disheartening here is how many figures that once stood by Pilger and his work, such as Amy Goodman and Chris Hedges, turned their backs on him as he sought to better understand Lannan's abrupt and inexplicable change of heart.[2]

Indeed, this instance illustrates the problems central to media that claim to be "radical" today: the immense power of such foundations is more than capable of exerting a stealth form of censorship and conformity that is close to impossible to accurately detect and gauge.

Further, the financial wherewithal of liberal foundations–Ford, Carnegie, Gates, OSI –far exceeds that of their conservative counterparts–Bradley, Olin, Scaife, Koch. What does that mean for the integrity of our information and opinion environments?

With these things in mind I waned to read a few observations made by Global Research editor and University of Ottawa Professor of Economics Michel Chossudovsky, who was unable to be on the panel this morning. His remarks are significant particularly in terms of charting the independent nature and trajectory of radical media today. Once you start receiving money from tax-free foundations," Chossudovsky notes in a GRTV interview,

… you lose your independence. We see it on the internet now. There are a number of internet [news] sites which look a little bit like the New York Times—the online version. They're still doing good work but they're becoming a little bit more politically correct.

So there's a mainstream alternative media and then there's an alternative media which I think is independent. There are not many, and that is the disturbing feature; many of the alternative media sites now are becoming corporatized. We want to avoid that. That's they're decision, but we have taken the decision that we do not seek any foundation funding which limits us from a budget point of view. It means that we [function] on a much more modest scale but we manage to be just as effective by doing that and we have the advantage of not being constrained to a particular perspective.[3]

How exactly does this dynamic play out in practical terms? Again, it is difficult to measure. Yet the FBI whistleblower Sibel Edmonds provides a clue. Edmonds notes how she received special guidance from foundation gatekeepers after she accepted money from a mainstream foundation as she was assembling a body of like-minded government insiders and whistleblowers.

Very quickly I realized that this money—these carrots they were dangling before our nose[s]—came with a bunch of string attachments. Because as I was talking with these people from these foundations I was adding more whistleblowers.

And in one case one [individual] from Clinton's previous administration joined the coalition who had blown the whistle on Al Gore and some narcotics-related case with the Drug Enforcement Agency. When I added this particular whistleblower—and he's still there on our list—these foundation people came and they said, "Why are you adding the Clinton administration whistleblower? Right now we are focused on [the] Bush administration. This is [a] distraction. And you should just limit [things] all this current wrongdoing and don't get in to all the Clinton stuff. Basically this is just one example of many *examples.[4]*

How perhaps does this dynamic play out at a more macro level? Two areas where there has not been enough serious intellectual activity and rigour of late is climate change and the crimes of 9/11, and it is truly amazing how so frequently the former is embraced by the left while the latter is dismissed–equally out of hand.

Think about it. The annual amount of foundation funding going toward publicizing forms of environmentalism is gargantuan.[5] There is, after all, a lot at stake: A new derivatives market, and setting up the "smart grid," both of which lay the groundwork for heightened government surveillance and eventually enforced austerity.

Is there any money devoted to a 9/11 truth commission or the equivalent? None. Is it discussed? Nope. How'd it happen? Blowback. Why is there a "war on terror" at home and abroad? They're protecting us from Al Qaeda.

9/11 is a root cause of a vast number of major problems in the body politic–war, the police state, the illicit drug trade, and on and on. At present, almost all roads lead back to it. What progressive outlets are discussing it? Global Research and Project Censored. How much foundation funding do they get? Practically none. Coincidence?

More than ever, the responsibility of intellectuals remains "speaking truth and exposing lies." Yet as the foregoing suggests, in the post-9/11 era particularly, the radical intellectual quest for "truth" itself has now become a commodity capable of being bought, sold and thus censored by some of the most wealthy entities on the planet. These murky forces do not just find the examination of topics like 9/11 unseemly; they also share an active interest in keeping them perpetually unexamined and suppressed.

Notes

[1] Noam Chomsky, "The Responsibility of Intellectuals," New York Review of Books, February 23, 1967.
[2] John Pilger, "Censorship That Dares Not Speak Its Name: The Strange Silencing of Liberal America," in Mickey Huff and Andy Lee Roth with Project Censored (editors), Censored 2014: The Top Censored Stories and Media Analysis of 2012-2013, New York: Seven Stories Press, 2013, 287-296. See also "The War You Don't See Pilger Film Banned By Lannan Foundation," Information Clearing House, June 10, 2011.
[3] Devon DB, "Michel Chossudovsky on the Creation of Global Research," GRTV, June 19, 2012.
[4] James Corbett, "The War on Whistleblowers: Sibol Edmonds on GRTV," GRTV, October 11, 2011.
[5] James F. Tracy, "The Forces Behind Carbon-Centric Environmentalism," MemoryHoleBlog, July 12, 2013.

LET'S RETHINK THE IDEA OF THE STATE: IT MUST BE A CATALYST FOR BIG, BOLD IDEAS

Mariana Mazzucato; The Observer; via Mark Barrett; Occupy

(It is true that a command economy can be made to work at least fairly well. Command economies were made to work tolerably well towards the closing stages of World War I and very well indeed on both sides of the Atlantic during World War II and since.
But what do we mean by 'the state' especially in a country which has a well-established love affair with enormous, bureaucratic and highly centralised institutional behemoths. As so often the item omits any consideration of institutional scale, subsidiarity and control. Switzerland manages to run high quality and institutionally stable health, education and transport systems without any central ministries devoted to any of those matters - Ed)

As George Osborne envisages a smaller state, economist Mariana Mazzucato argues instead that a programme of forward-thinking public spending is crucial for a creative, prosperous society. We must stop seeing the state as a malign influence or a waste of taxpayers' money

In his epic book, The End of Laissez-Faire (1926), John Maynard Keynes wrote a sentence that should be the guiding light for politicians around the globe. "The important thing for government is not to do things which individuals are doing already, and to do them a little better or a little worse; but to do those things which at present are not done at all."

In other words, the point of public policy is to make big things happen that would not have happened anyway. To do this, big budgets are not enough: big thinking and big brains are key.

While economists usually talk about things that are not done at all (or done inadequately) by the private sector as "public goods", investments in "big" public goods like the UK national health service, or the investments that led to new technologies behind putting a "man on the moon", required even more than fixing the "public good" problem. They required the willingness and ability to dream up big "missions". The current narrative we are being sold about the state as a "meddler" in capitalism is putting not only these missions under threat, but even more narrowly defined public goods.

Public goods are goods whose benefits are spread so widely that it is hard for business to profit from them (or stop others profiting from them). So they don't attract private investment. Examples include transport infrastructure, healthcare, research and education.

Even if you're an avid free-marketeer you can't avoid benefiting, directly and indirectly, from such public investments. You gain directly through the roads you drive down, the rules and policing which ensure their safety, the BBC radio you listen to, schools and universities that train the doctors and pilots you depend on, parks, theatre, films and museums that nurture our national identity. You also gain, indirectly, through enormous public subsidies without which private schools, hospitals and utility providers would never be able to deliver affordably and still make a profit. These are conferred as tax breaks, and provision of vital skills and infrastructure at state expense.

While social welfare is relentlessly trimmed and targeted, corporate welfare grows inexorably, as business widens its relief from the taxes that fund public infrastructure (while tax credits top-up its less generous wage packets). And the non-appropriable benefits of knowledge – costly to produce, cheap to acquire and use once published – spread the influence of public goods much wider. Nuclear fusion, fuel cells, asset-pricing formulas and genome maps are discoveries for all, not just one company. But it now seems like the doubters, those who contest the idea of "public goods", have won the contest. The state's provision of many of these goods – notably transport, education, housing and healthcare – is being privatised or outsourced at an increasing rate. Indeed privatisation and outsourcing are happening at such a rapid pace in the UK they are practically being given away – as the sale of Royal Mail at rock bottom prices revealed recently – denying the state a return for its near-century long investment.

Yet because we are told the state is simply a "spender" and meddling "regulator", and not a key investor in valuable goods and services, it is easier to deny the state a return from its investment: risk is socialised, rewards privatised. This not only eliminates any return on public investment but also destroys institutions that have taken decades to build up, and rapidly erodes any idea of public service distinct from private profit.

When public goods are privatised they lose their "public good" nature: it does become possible to profit from distributing mail, running trains, renting out homes and providing education. We're continually promised that, due to efficiency gains and innovations prompted by the profit motive, public goods can be delivered more cheaply and effectively by the private sector. All this while still giving their providers a decent profit, so that more is invested.

Has privatisation of UK rail provided lower prices, more innovation and investment? Has contracting-out prison security to G4S made that system more efficient and high quality? Have outsourced NHS services provided the taxpayer with higher quality healthcare that's still free of charge and assigned on merit? Users' impressions and regulators' performance indicators give at best a mixed signal on service quality. Private firms' commercial confidentiality – often a stark contrast with the right-to-know approach to public enterprise – makes it hard to identify or measure any changes in efficiency.

So the state is robbed of its deserved returns of investment, and public services are worsening – but is the state at least relieved of the associated costs and financial burden? No. What's very clear is that while private profits are now being made, public subsidy has not disappeared. The UK government explicitly subsidises its "privatised" utilities, with net transfers amounting to (among others) more than £2bn annually for train operating companies, and £10bn in investment guarantees alone for new nuclear power station builders (these, ironically, include other countries' state-owned utility firms – willing to advance their capital under the generous long-term price arrangements offered by the government, while their privatised UK counterparts like Centrica dismiss these as too risky and return their cash to shareholders).

Private companies can receive further implicit subsidies through investment guarantees and tax breaks; ad hoc assistance (such as meeting energy firms' decommissioning costs, and taking over pension liabilities to enable privatisation, as with Royal Mail and the remnants of the coal industry); rules that enable the circumvention of corporate taxes that are already below income-tax rates (and falling fast); and the assurance that the state will step back in to repossess (without penalty) any operations the private sector finds too expensive, as with Network Rail and the East Coast train-operating franchise.

But in the US, UK and all across Europe, where it's almost universally argued that today's governments are too big, these subsidies are rarely called into question. The debate focuses on the need for public debt levels to come down. And since taxes are judged to be too high – on the basis of very unclear arguments regarding incentives – debt reduction ends up relying on massive public-spending cuts. Growth will supposedly be stimulated by reducing the size of the public sector though privatisation and outsourcing – alongside the eternally-promised reduction of tax and "red tape", which is seen to be hindering an otherwise dynamic private sector.

Typically, the last UK budget focused on targeted tax reductions which are more fairly termed "tax expenditures", lifting a "burden" from companies that other sectors (mainly public services) will have to absorb. These include a drop in corporation tax to 20% from April 2015 (explicitly designed to undercut the rest of the G20), more reliefs from national insurance, and reductions in regulation – always hailed as reducing cost, despite the financial sector's recent warning on where those short-term savings can later lead.

Is tax too high? In the US, the top marginal income tax rate was close to 90% under Republican president Dwight Eisenhower – widely recognised as reigning over one of the highest growth periods in US history. Today the total US tax bill is the lowest it has ever been. The spending cuts about to hit the US – the infamous "sequester", which will damage institutions ranging from NASA to social services – would not be needed if the US tax bill (24.8% of GDP) were only four percentage points lower than the OECD average (33.4%), instead of eight points.

Yet tax cuts usually achieve no discernible increase in investment, only a measurable increase in inequality. This is because what actually guides business investment is not the "bottom line" (costs, as affected by tax) but anticipation of where the future big technological and market opportunities are.

In the UK, Pfizer did not move its largest R&D lab in Sandwich, Kent to Boston due to lower tax or regulation but due to the £32bn a year that the US National Institutes of Health (NIH) spends on the bio-medical knowledge base that feeds them. Equally, although it was the National Venture Capital Association that in the mid-1970s negotiated huge reductions in US capital gains tax (from 40% to 20% in just six years), venture capital was actually following the footsteps of strategic public funding. In biotech, it entered the game 15 years after the state did the hard stuff.

And when the UK's Labour government reduced the minimum time for private equity investment to qualify for similar tax breaks from 10 to two years,it made venture capital even more short-termist, increasing golfing time not investing time. For the private sector, opportunities lie not in the creation of major new knowledge and technology but in the returns on investment in "intellectual property" that others have commissioned and not yet commercialised. Profit flows from privately capturing the "external benefits" conferred by public goods, when the public sector continues to underwrite them

The challenge today is to bring back knowledge and expertise into government that can drive the big missions of the future. Yet current de-skilling and de-capacitating government will not allow that. As I discuss in my new book, The Entrepreneurial State: debunking private vs. public sector myths, all the technologies that make the iPhone so smart were indeed pioneered by a well-funded US government: the internet, GPS, touch-screen display, and even the latest Siri voice-activated personal assistant.

All of these came out of agencies that were driven by missions, mainly around security – and funding not only the upstream "public good" research but also applied research and early-stage funding for companies. New missions today should be expanded around problems posed by climate change, ageing, inequality and youth unemployment. But while it's great that Steve Jobs had the genius to put those government technologies into a well-designed gadget, and great, more generally, for entrepreneurs to surf this publicly funded wave, who will fund the next wave with starved public budgets and a financialised and tax-avoiding private sector?

As the late historian Tony Judt used to stress, we should invent and impose a new narrative and new terminology to describe the role of government. The language being used to describe government activity is illuminating. The recent RBS sale was depicted as government retaining the "bad" debt, and selling the "good" debt to the private sector. The contrast could not be starker: bad government, good business – a needless inversion of the public good.

And public investments in long-term areas like R&D are described as government only "de-risking" the private sector, when actually what it is doing is actively and courageously taking on the risk precisely where the private sector – increasingly more concerned with the price of stock options than long-run growth opportunities – is too scared to tread. Once the entrepreneurial and risk-taking role of government is admitted, this should result in a sharing of the rewards – whether through equity of retaining a golden share of the patent rights. By privatising public goods, outsourcing government functions, and the constant state bashing (government as "meddler", at best "de-risker") we are inevitably killing the ability of government to think big and make things happen that otherwise would not have happened. The state starts to lose its capabilities, capacity, knowledge and expertise.

Examples that counter this trend – and language – should be celebrated. When the BBC invested in iPlayer – the world's most innovative platform for online broadcasting – instead of outsourcing it, it went against the grain. It brought brains and knowledge into a public sector institution. When recently the Government Digital Services (GDS) – part of the UK's Cabinet Office – wanted to create its own website, the usual solution was to outsource it to Serco, a private company that has recently won many government contracts (even Obamacare insurance work).

Dissatisfied with the mediocre site that Serco offered, GDS brought in coders and engineers with iPlayer experience, who went on to produce an award-winning website that is costing the government a fraction of what Serco was charging. And in so doing also made government smarter – attracting, not haemorrhaging, the knowledge and capabilities required for dreaming up the missions of the future.

To foster growth we must not downsize the state but rethink it. That means developing, not axing, competences and dynamism in the public sector. When evaluating its performance, we must rediscover the point of the public sector: to make things happen that would not have happened anyway.

When the BBC is accused of "crowding out" private broadcasters, the difference in quality of the programmes is considered a subjective issue not worthy of economic analysis. Yet it is only by observing and measuring that difference that we can accurately judge its performance. The same is true for the ability of public sector institutions not only to subsidise pharmaceutical companies but actually to transform the technological and market landscape on which they operate.

The public sector must produce public goods, and through the creation of new missions catalyse investment by the private sector – inspiring and supporting it to enter in high-risk areas it would not normally approach. To do so it requires the ability to attract top expertise – to "pick" broadly defined directions, as IT and internet were picked in the past, and "green" should be picked in the future. Some investments will win, some will fail. Indeed, Obama's recent $500m guaranteed loan to a solar company Solyndra failed, while the same investment in Tesla's electric motor won big time – making Elon Musk richer.

But as long as we admit the state is a risk-taking courageous investor in the areas the private sector avoids, it should increase its courage by earning back a reward for such successes, which can fund not only the (inevitable) losses but also the next round of investments. Instead, calling it names for the losses, ignoring the wins, and outsourcing the competence and capabilities, is ridding it of the courage, ability and brains to create the missions, hence opportunities, of the future. And without brains, all government will be able to do is not make big things happen but simply serve a private sector that is concerned only with serving itself.

Mariana Mazzucato is Professor in the Economics of Innovation at the University of Sussex, and author of The Entrepreneurial State: debunking private vs. public sector myths (Anthem, 2013)

BOOK REVIEW; ELLEN BROWN 'THE PUBLIC BANK SOLUTION'

Tony Crawford; via Global Table and Common Futures

'The Public Bank Solution' subtitle, 'From Austerity to Prosperity' is an outstanding history of money, notable bankers through the ages, and banking methods behind and beyond the 2008 Global Credit Crunch. The writer is Ellen Brown J. D., US Attorney, president of Public Banking Institute and author of several books.

If my postgrad professor had wanted a 'The Public Bank Solution' book report for a scholarly grade, a study of money according to Ellen Brown would have changed my life. I would have become wary of bankers knowing they had subjugated financial institutions at home and abroad, as well as plundered vanquished banks of war conquered nations. I would have known more about bank moneymaking schemes, and how to avoid debt to avaricious people with insatiable greed for money and abnormal hatred of parting with it.

Ellen Brown is a must read for anyone wanting self-preservation in a seriously tilted world for bankers.

The author analyses money that unfolds in marvellous detail of what filthy lucre is, and where it goes. A review by way of an introduction might caution, "Don't tell me the ending." But in this case, the author has written for people like me… that we might never know what's been missed, until it's gone, in the last chapter.

Brown's book paints a picture of a most government subsidized industry on the planet. Politicians of all stripes appear to champion capitalistic private banks over altruistic public banks. It is a study of socioeconomic trials of national monetary policy under constant pressure from international banks for a new world order. It sets public and private bankers apart like 'Jekyll and Hyde' split personalities: Publicly-owned banks operate in the public interest by law; privately-owned banks make and use law solely for purpose of privatized gains from socialized losses that governments seem willing, if not wilful, to bestow deficit economies upon its taxpayers.

The volume starts with an overview of how banks work and where money earned as wages duly taxed comes from. Ancient clay tablets counted transaction types in trade as the first evidence of money long before metal coins and papered credit to banknotes. China used papered notes as money since the tenth century that Marco Polo described from his travels in the Orient. England had a wooden 'Tally Stick' version of money that was used to settle tax as duty owed King Henry the First around the twelfth century. Money emerged as coins and banknotes across Europe that banks portrayed with sovereign face-value received from credit in numbers counted as money that bankers lent to agreeable debtors.

The book describes a bank revolution that started with Italian zero-balance double-entry bookkeeping invented in the thirteenth century that became standard practice across Europe in the fifteenth. Positive numbers for bank deposits were counted to balance with a zero difference to negative numbers for bank overdrafts secured by gold in reserve. Credit used was reckoned as money from debt that charged interest for the cost of money. Fudged numbers spawned more money from higher quotients of loans to deposits. Savings on the credit side were bank liabilities that paid interest on principal until paid out, on demand. Loans on the debit side were bank assets that charged interest terms and conditions until principal collected in, on demand. When credit exceeded deposits it magically created money from a less than zero negative difference that was a breach of protocol. Indeed, bankers who were tempted and failed to collect debt as money were sent to jail and even hanged for not holding deposits in full reserve, which was gold in those days. Italian banks also developed Bills of Exchange that any person with adjudicated credit could order another person, or a bank, to honour a signed note, dated and filled out for money to pay a third party. The medieval system of cheques that moved paper instead of gold became accepted as currency. It involved a central clearing function to balance credit carried in trust between banks. The benefit of personal credit added to the money supply stimulated trade and economic growth. The 'Checkbook Money' system allowed people to handle IOU promises as if money. The more personal credit, the less physical gold banks had to move in trade. It meant holding less precious metal in bank vaults than total deposit value. The bank crafted number was an increased ratio for a lower so-called 'fractional reserve'.

Banking methods spread further afield and credit crossed international boundaries that made products and services in multiple currencies to manage. The Bank of Sweden created the first private Central Bank under government control in 1668. The UK government followed in 1694 with a charter that financiers could operate the Bank of England as a private Central Bank authorized to print national banknotes as legal tender. The UK was the first government to carry national deficits to private creditors funding war from never-ending debt that taxpayers paid interest on permanent loans constantly rolled over in perpetuity. English Law was the first to enforce 'fractional reserve' that the Central Bank could print more money than gold its notes promised to pay all its bearers on demand. Westernised nations adopted similar rules in Bank Acts round the world.

In Europe, France created a Central Bank in 1803 and sovereign nations did the same through the nineteenth century. In the USA, President Taft authorized income tax and President Wilson saw the Federal Reserve Bill into law in 1913. In 1929, a Central Bank was created to handle First World War reparations called the BIS - the Bank for International Settlements. It still watches over national Central Banks that oversee domestic banks. Money was pegged to a 'Troy ounce' of gold from 1944 until 1971 when US President Nixon removed the US Dollar from the 'Gold Standard'. The USA pushed all reserve currencies into 'fiat' money that paper as money the world over became legal tender only due to a Latin meaning for something done, 'fiat - let it be'.

Modern banks continue to use four hundred year old medieval math with ever increasing computer lightning speed and massive volume. The author reviews the actions of the BIS, FSB - Financial Stability Board, and IMF - International Monetary Fund as 'exotic' derivatives emerged from deregulation until the largest seizure in 2008 of a global financial conduit in history. Layers of governance and political spins give an impression of control for public good, but the writer is not optimistic about public banks in the big picture.

'The Public Bank Solution' is a compelling read about the dark secrets of banking. Brown dispels any doubt that public banks differ from private banks with clear examples. North Dakota is the only state that owns its own bank in the USA. Its monetary policy saved it from worsening debt in the financial crisis in 2008. But not so the Bank of Canada, which is the only publicly-owned Central Bank in the G20. Quote Page 204: "… private banks create the money they lend just the same as public banks do. The difference is that a publically-owned bank returns the interest to the government and the community, while a privately-owned bank siphons it into private accounts, progressively drawing money out the productive economy." 1974 saw the end of Canadian self-funded credit to print its own money when the BIS established 'Financial Stability' policy that all governments must borrow from private global banks. Quote Page 207: "Thus in 1993, 91 percent of the debt consisted of interest charges… By 2012, the government had paid C$1 trillion in interest - twice its national debt."

Brown's history of finance reads like a crime novel that ends with the biggest heist in the world. UK Barclays Bank denied criminal acts in the LIBOR - London Interbank Offered Rate scandal that it rigged the cost of money to profit from so-called 'exotic' financial products. The innovation of notional value received from imaginary credit in the workings of mortgage derivatives triggered financial ruin at the turn of the twentieth century. It is not fiction. World governments recapitalized banks in debt to trillions at taxpayers' expense. Nonfiction starts, quote Page 25, "The shadow banking system has allowed the private expansion of credit by piling debt upon debt in a fragile house of cards that is mathematically unsustainable. Operating outside the prying eyes of bank regulators, the shadow system allows credit to be generated without regard to capital requirements, reserve requirements, or the need to balance loans (assets) against liabilities (deposits), as conventional banks must do."

Doing as conventional banks must do is a distant thing of the past. Ellen Brown has written a fascinating book that was a gift to me. I can't pass it on. It's a constant reminder of usurism I can't believe is banking. My volume is reread, dog-eared, coffee stained, and splotched from felt-tip markers. If I meet the author, I want it signed, "To Tony, Canadian citizen and proud owner of the Public Bank of Canada" Ellen Brown.

POSTIVE MONEY BULLETIN

Ben Dyson; Positive Money Team

In September this year Scotland will vote on whether to become independent from the rest of the UK. Whatever the outcome of that referendum, it has sparked a huge amount of interest and debate about what currency Scotland should use. A major question concerns which currency an independent Scotland would use: the pound, the euro, or a new Scottish currency? This is a really exciting time to be talking about money reform and to build a strong movement - and we invite you to become a part of it:

If an independent Scotland wished to establish its own currency, there is little sense in modelling the currency on a design that has already spectacularly failed many times in the UK, Europe and the US. There is a better way which would give Scotland a safer banking system and an economy that is more stable and far less dependent on debt, a system where badly-run banks could be allowed to fail.

Read our new report:

"A Scottish Currency? - 5 Lessons from the Design Flaws of Pound Sterling"

Upcoming Events

Fri 7th March, London - Loconomics Workshop 1
Fri 14th March, London - Loconomics Workshop 2
Fri 21st March, London - Loconomics Workshop 3
Fri 28th March, London - Loconomics Workshop 4

More from the Blog

House prices: If wages had kept up, we'd earn £44,000 more
Hair of the dog risks a bigger hangover for Britain (FT)
Should we accept the world's banks can do what they like? (Ben Dyson on BBC World Service)
Adair Turner: Escaping The Addiction to Private Debt Is Essential for Long-Term Economic Stability
NEW DOCUMENTARY - Enough is enough (Full Film, 18 min)
What is Money?…and Why Does it Matter? (Video)
The Guardian: Change to UK's money system could solve our long-term economic problems
How to fix the creation of money?
Would Positive Money reform lead to a reduction in credit available to businesses?
"Finding Shelter" – How the UK Property Market Became an Investment Vehicle for the Global Super-Rich
My flat earns so much more than I do…

2014 is already shaping up to be an exciting year. Last week The Guardian featured an article by Ben

Dyson on the need to reform the monetary system - a great breakthrough into the British press.

We are in the Guardian

“Oh, at long last the monetary reform movement gets a long overdue platform in the Guardian. This is the biggest story out there right now – shamefully untold by the British media and the greatest opportunity for the ordinary people of this nation to improve their lot that exists today. I’m so delighted to see Ben and Positive Money get some coverage – what that small team has achieved with shoestring resources is little short of miraculous – every right thinking person should go and visit their website right now."

This is one of many comments below Ben Dyson’s article entitled “Change to UK’s money system could solve our long-term economic problems” in the Guardian on Wednesday 6th Feb 2014

Thanks to everyone who donated to help bring Martin Campbell on board the PM team. Get involved in the next steps of the campaign by coming to our conference - get your ticket here.

Results of Positive Money supporters' survey

A big thank you to the 1293 people who took part in our supporter survey, it has been very useful to find out about you! Here are a few stats:

27% of Positive Money supporters are self-employed
42% people became interested in the monetary system because of inequality
15% found out about Positive Money through a friend
47% people think that eventually banks will be prevented from creating money, but 54% think that we need another financial crisis before anything will be changed
56% people think that the most important change we will see with our reforms is equality and social justice

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