China Rolls Out Big Brother Technocracy On Citizens

Digital slavery and Scientific Dictatorship are straight ahead for all of China, which has been moving toward Technocracy for at least 25 years. Punishment for non-compliance will be instant, irrevocable and non-transparent. Much of the technology being used in supplied by Western companies that are legally blocked by their home countries, but not so forever. Thus far, Americans are not at all alarmed that these systems will soon be applied to them. □ TN Editor

> *It was a drab, chill day in November, and the clocks were striking thirteen. As the woman passed through Hangzhou Railway Station, she moved quickly through the ticket gates—though not quickly enough to avoid detection by the transport authority, which noticed her failure to swipe the correct transit pass. It was too late. She had received a black mark on government records that would make it harder than ever for her to travel in the future.*

That's a reimagining of the introduction to George Orwell's dystopian novel *Nineteen Eighty-Four*. But it's also set to become a reality for citizens of China if the government's dream of an authoritarian big-data scheme comes to fruition.

The *Wall Street Journal* reports that the Chinese government is now testing systems that will be used to create digital records of citizens' social and financial behavior. In turn, these will be used to create a so-called social credit score, which will determine whether individuals have access to services, from travel and education to loans and insurance cover. Some citizens—such as lawyers and journalists—will be more closely monitored.

Planning documents apparently describe the system as being created to "allow the trustworthy to roam everywhere under heaven while making it hard for the discredited to take a single step." The *Journal* claims that the system will at first log "infractions such as fare cheating, jaywalking and violating family-planning rules" but will be expanded in the future—potentially even to Internet activity.

Some aspects of the system are already in testing, but there are some challenges to implementing such a far-reaching apparatus. It's difficult to centralize all that data, check it for accuracy, and process it, for example—let alone feed it back into the system to control everyday life. And China has data from 1.4 billion people to handle.

As the *Financial Times* reported earlier this year, it's not currently well-equipped to do so. Speaking about the nation's attempts to probe citizen data to measure creditworthiness, Wang Zhicheng of Peking University's Guanghua School of Management told the newspaper, "China has a long way to go before it actually assigns everyone a score. If it wants to do that, it needs to work on the accuracy of the data. At the moment it's 'garbage in, garbage out.'"

Not that such issues are likely to stop officials from pursuing such a goal. The nation's citizens already have to deal with strict Internet censorship, and Jack Ma, the founder of Chinese e-commerce site Alibaba, recently called on the government to use sweeping data analysis to identify criminals.

If China can work out how to corral its data across government departments, cities, and districts, the scoring system will simply be another Big Brother tactic in the nation's increasingly totalitarian approach to governance.

Software Giant Oracle Launches ‘Smart City In A Box’

The computer titans of the world are rushing to get their share of the multi-trillion dollar market for automation of Smart Cities. This is the essence of Scientific Dictatorship because the UN’s New Urban Agenda calls for complete geo-spatial monitoring of everything within a city. □
TN Editor

State governments have been working to get their Smart City projects off the ground for sometime. While technology will be the enabler for services, states have to spend on creating infrastructure initially. While some cities are still creating Special Purpose Vehicles (SPVs), others have moved ahead to bring out request for proposal (RFP) to implement the projects. Maharastra which has 10 cities government signed a memorandum of understanding (MOU) with Oracle. Niraj Prakash, director, solution consulting, Oracle India spoke to Anup Jayaram on the Smart City initiave.

Q: What does the MoU that you signed with Maharashtra on

Smart Cities entail?

A: The MoU that we signed with Maharashtra in the US is a way forward on a partnership that we want to create with government. We will create a centre of excellence (CoE), which can help generate solutions around modern government. The CoE which will be located in a government of Maharashtra premises or real estate is where we can test and develop newer solutions which can help in Smart Cities. It will leverage cloud solutions and entrepreneurs can come and test newer solutions there. The internet of things (IoT) is a new technology and there are numerous use cases. You need to connect the new technology with the use case to see what works best and has maximum impact on citizens.

Q: Oracle has partnered with many cities globally. What learnings can you bring here?

A: Oracle has hundreds of cities globally as strong customers. We worked in Los Angeles, Atlanta, New York and the Middle East. Across the world we have done a lot of IT transformation. That gives us an enormous understanding of what cities are, what kind of transformation can happen and what do they impact. Today we are looking at how to embed an IoT component, mobile, social and big data components in the offering.

Q: What is the status of Smart Cities now?

A: Once a city is identified, it has to create a special purpose vehicle (SPV), followed by an organization structure and a CEO. Then it needs to identify a managed service partner (MSP) who will look at the city and see what greenfield and brownfield areas are there and what it wants to prioritise. Then they will float RFPs to identify system integrators (SIs) to implement that. Many cities are busy doing that. Pune, Raipur and Nagpur have come out with RFPs. While these cities have moved faster, others are getting their SPVs in place.

Q: While technology is key, isn’t infrastructure a bigger issue in Smart Cities?

A: Yes, that’s true. Public safety, transportation, parking and solid waste management are among the seven common priorities across cities. In waste management some cities want bins, but in others there are plans to remove garbage bins totally; they will collect it from the source. Parking is an issue across cities. Smart parking involves an IT component, but space has to be created. Then you need sensors at each parking slot. That data has to be moved to a central command centre. There is civil and IT infrastructure involved. Then comes the IT backbone on top of which it is going to ride. A large part of the cost would be incurred in the civil construction cost for the parking.

Q: What are the challenges?

A: Smart cities requires a balance between distributed architecture, distributed IT systems and a convergence of IT systems. It's a combination of distribution and converged systems. This distribution is not simple: every bus, mobile and sensor has to have it. Managing this immense distribution is important. The solution vendors are small parties and will come with their own technology piece which is proprietary to them. We recommend a common IoT backbone. While all along the command centre has been owned by say the police, or by the municipality, that's not the way to do it. You will need a common command centre with different domains.

Q: How is Oracle changing this?

A: We are offering a one stop shop—Smart City in a Box. What we are trying to do is partner with some of niche solution providers in transportation, parking and waste management and get their application on to this particular box. This is an opex box, which means there is no capex but you pay as you use. We will put in partner applications and our applications like billing, real estate management, citizen services in this box and pay as you use. It is a recommended solution that we have created. We are discussing with many state governments.

Surveillance Industry Eyeing Huge Profits Under A Trump Presidency

Lobbyists for the surveillance industry already smell big profits ahead, thanks to Trump. For instance, the designated CIA appointee, Rep. Mike Pompeo, is a major proponent of the surveillance society and will provide many expansion opportunities. The chosen National Security Advisor, Gen. Michael Flynn, is also favorable on surveillance expansion. TN Editor

As the looming specter of a Donald Trump presidency continues to terrify minority groups throughout the United States, one industry is greeting the new administration with open arms.

Speaking at a physical surveillance trade show on Wednesday, two representatives from the Security Industry Association (SIA) – which lobbies the government on behalf of surveillance tech manufacturers – laid out the myriad ways Trump could be great news for their members' bottom line. Overall, the near-certainty that Trump will increase spending on defense border security means it's a great time to be in the surveillance world.

Jake Parker, the director of government relations at SIA, and Joe Hoellerer, manager of government relations at SIA, spoke at a side event during ISC East, the largest physical surveillance trade conference in the northeast. SIA represents about 700 different companies, and although Trump hadn't announced any cabinet appointments yet, Parker addressed some of the names that had been floated.

"Congressman [Michael] McCaul is on the shortlist for DHS Secretary. He's someone who has been very active, very supportive of our industry, so that would definitely be great if that happened." Parker said.

McCaul is current the chairperson of the House Committee on Homeland Security, and should he get the nod to head DHS, he will almost certainly be criticized by human rights groups for his stance on militarizing the southern border and other civil liberties issues.

Parker also discussed Senator Jeff Sessions, who Trump later picked for Attorney General, noting that Sessions "spoke at the [SIA] government summit this last year." In a press release announcing that Sessions would address the summit, SIA CEO Don Erickson offered the below statement:

> *I can think of no lawmaker more involved in issues of paramount importance to the security industry today, and I anticipate the senator will have thought-provoking insights to share with conferees at the SIA Government Summit.*

Read full story here…

Britain Ends All Privacy By Passing The ‘Snooper Charter’

While Brits think Brexit will solve their ‘Big Brother’ problems, they completely miss that they are being directly controlled by Technocrats, the chief of which is their current Prime Minister, Theresa May. The ‘end of privacy’ means 100 percent knowledge about every citizen – and knowledge is power. TN Editor

Britain has passed what everyone calls the “snooper’s charter” otherwise known as the Investigatory Powers Bill.

This new legislation establishes the legal framework authorizing the government to hack into devices, networks and services in bulk and to create vast databases of personal information on all UK citizens. This is a preliminary step for a movement to impose worldwide taxation on Brits.

This is really to hunt money, not terrorism.

The “snooper’s charter” requires internet, phone and communication app companies to store records for 12 months and allow authorities to access them whenever they demand. That data will include anything you look at or search on the internet as well as all your telephone calls and text messages. Meanwhile, security agencies will be able to force companies to decrypt data avoiding the Apple confrontation in the USA. They are also imposing limitations on the use of end-to-end encryption.

They want EVERYTHING you do. This has ABSOLUTELY nothing to do with terrorism.

This is the hunt for taxes coming to a head in 2017.

Hacking power

For the first time, security services will be able to hack into computers, networks, mobile devices, servers and more under the proposed plans. The practice is known as equipment interference and is set out in part 5, chapter 2, of the IP Bill.

This could include downloading data from a mobile phone that is stolen or left unattended, or software that tracks every keyboard letter pressed being installed on a laptop.

"More complex equipment interference operations may involve exploiting existing vulnerabilities in software in order to gain control of devices or networks to remotely extract material or monitor the user of the device," a draft code of conduct says.

The power will be available to police forces and intelligence services. Warrants must be issued for the hacking to take place.

Bulk hacking

For those not living in the UK, but who have come to the attention of the security agencies, the potential to be hacked increases. Bulk equipment interference (chapter 3 of the IP Bill) allows for large scale hacks in "large operations".

Data can be gathered from "a large number of devices in the specified location". A draft code of practice says a foreign region (although it does not give a size) where terrorism is suspected could be targeted, for instance. As a result, it is likely the data of innocent people would be gathered.

Security and intelligence agencies must apply for a warrant from the Secretary of State and these groups are the only people who can complete bulk hacks.

Commissioners

To help oversee the new powers, the Home Office is introducing new roles to approve warrants and handle issues that arise from the new powers. The Investigatory Powers Commissioner (IPC) and judicial commissioners (part 8, chapter 1 of the IP Bill) will be appointed by Theresa May, or whoever the serving prime minister is at the time.

The IPC will be a senior judge and be supported by other high court judges. “The IPC will audit compliance and undertake investigations,” the government says.

“The Commissioner will report publicly and make recommendations on what he finds in the course of his work,” guidance on the original bill says (page 6). “He will also publish guidance when it is required on the proper use of investigatory powers.”

Web records

Under the IP Bill, security services and police forces will be able to access communications data when it is needed to help their investigations. This means internet history data (Internet Connection Records, in official speak) will have to be stored for 12 months.

Communications service providers, which include everything from internet companies and messenger services to postal services, will have to store meta data about the communications made through their services.

The who, what, when, and where will have to be stored. This will mean your internet service provider stores that you visited WIRED.co.uk to read this article, on this day, at this time and where from (i.e. a mobile device). This will be done for every website visited for a year.

Web records and communications data is detailed under chapter 3, part 3 of the law and warrants are required for the data to be accessed. A draft code of practice details more information on communications data.

Bulk data sets

As well as communications data being stored, intelligence agencies will also be able to obtain and use "bulk personal datasets". These mass data sets mostly include a "majority of individuals" that aren't suspected in any wrongdoing but have been swept-up in the data collection.

These (detailed under part 7 of the IP Bill and in a code of practice), as well as warrants for their creation and retention must be obtained. "Typically these datasets are very large, and of a size which means they cannot be processed manually," the draft code of practice describes the data sets as. These types of databases can be created from a variety of sources.

Finally, we leave it to Edward Snowden to summarize just how insane this bill is…

> *The UK has just legalized the most extreme surveillance in the history of western democracy. It goes farther than many autocracies.* https://t.co/yvmv8CoHrj
> — Edward Snowden (@Snowden) November 17, 2016

Julian Assange On Google: They ‘Do Things The CIA Cannot’

Eric Schmidt, Executive Chairman of Google, is a member of the elitist Trilateral Commission that has promoted Technocracy since 1973. Schmidt is fully enmeshed in transforming the world according to the Technocrat vision. TN Editor

Julian Assange cautioned all of us a while back, in the vein of revelations similar to those provided by Edward Snowden, that Google — the insidious search engine with a reputation for powering humanity’s research — plays the dark hand role in furthering U.S. imperialism and foreign policy agendas.

Now, as the Wikileaks founder faces days of questioning by a Swedish special prosecutor over rape allegations inside his Ecuadorian Embassy haven in London today — and particularly in wake of the presidential election — Assange’s warning Google **“is not what it seems”** must be revisited.

Under intense scrutiny by the U.S. State Department for several controversial Wikileaks' publications of leaked documents in 2011, Assange first met Google Executive Chairman, then-CEO, Eric Schmidt, who approached the political refugee under the premise of a new book. Schmidt, whose worth *Forbes* estimates exceeds $11 billion, partnered with Council on Foreign Relations and State Department veteran, Jared Cohen, for the work, tentatively titled *The Empire of the Mind* — and asked Assange for an interview.

Later acknowledging naïvte in agreeing to meet the pair of tech heavyweights, Assange found afterward how enmeshed in and integral to U.S. global agendas Schmidt and Cohen had become.

In fact, both have exhibited quite the fascination with technology's role in burgeoning revolutions — including, but not-at-all limited to, the Arab Spring. Schmidt created a position for Cohen in 2009, originally called Google Ideas, now Google Jigsaw, and the two began weaving the company's importance to the United States into narratives in articles, political donations, and through Cohen's former roles at the State Department.

That same year, Schmidt and Cohen co-authored an article for the CFR journal Foreign Affairs, which, seven years hence, appears a rather prescient discussion of Google's self-importance in governmental affairs. Under the subheading "COALITIONS OF THE CONNECTED," they wrote [all emphasis added]:

*"In an era when the power of the individual and the group grows daily, **those governments that ride the technological wave will clearly be best positioned to assert their influence and bring others into their orbits.** And those that do not will find themselves at odds with their citizens.*

***"Democratic states that have built coalitions of their militaries** have the capacity to do the same with their connection technologies. […] they **offer a new way to exercise the duty to protect citizens** around the world who are abused by their governments or barred from voicing* *their opinions."*

Perhaps appearing laudable on its surface — at least to some degree — as Assange pointed out, there is a self-mischaracterization by the American and other Western governments and inaccurately-monikered 'non-governmental organizations' that their interests in other nations' affairs are innately good.

This cult of government and non-government insiders have a firm belief their goals should be the unassailable, unquestionable motivator for American imperialism — whatever the U.S. thinks best as a "benevolent superpower," so should the rest of the 'non-evil' world.

"They will tell you that open-mindedness is a virtue, but all perspectives that challenge the exceptionalist drive at the heart of American foreign policy will remain invisible to them," Assange wrote in *When Google Met Wikileaks*. ***"This is the impenetrable banality of 'don't be evil.' They believe that they are doing good. And that is a problem."***

Cohen, an Adjunct Senior Fellow at the notorious Council on Foreign Relations, lists his expertise in *"terrorism; radicalization; impact of connection technologies on 21st century statecraft; Iran,"* and has worked for both Condoleezza Rice and Hillary Clinton at the Department of State. *Fortune*, calling Cohen a *"fascinating fellow,"* noted that, in his book *Children of Jihad*, the young diplomat and technology enthusiast ***"advocates for the use of technology for social upheaval in the Middle East and elsewhere."***

Under the auspices of discussing technological aspects at Wikileaks' disposal for the upcoming book, Schmidt; Cohen; Lisa Shields, a CFR vice president at the time; and Scott Malcomson — who would shortly afterward be appointed Rice's lead speech advisor for her role as the U.S. ambassador to the United Nations — descended on Assange's safe haven in Norfolk, outside London.

It wasn't until weeks and months after this gathering Assange fully realized how closely Google operates in tandem with the government of the United States — and how perilous the innocent mask of its public intentions truly is in light of such cooperation.

Ironically enough, in Wikileaks' publishing three years later of the Global Intelligence Files — internal emails from private security firm, Stratfor — Cohen's and Google's true depth of influence became strikingly apparent. Assange wrote:

> ***"Cohen's directorate appeared to cross over from public relations and 'corporate responsibility' work into active corporate intervention in foreign affairs at a level that is normally reserved for states. Jared Cohen could be wryly named Google's 'director of regime change.'*** *According to the emails, he was trying to plant his fingerprints on some of the major historical events in the contemporary Middle East. He could be placed in Egypt during the revolution, meeting with Wael Ghonim, the Google employee whose arrest and imprisonment hours later would make him a PR-friendly symbol of the uprising in the Western press. Meetings had been planned in Palestine and Turkey, both of which—claimed Stratfor emails—were killed by the senior Google leadership as too risky. Only a few months before he met with me, Cohen was planning a trip to the edge of Iran in Azerbaijan to 'engage the Iranian communities closer to the border,' as part of Google Ideas' project on repressive societies."*

Read full story here…

It Begins: China's Premier Speaks Out On Global Governance Of Internet

China's Technocrat Premier Xi Jinping is first out of the gate to make a global statement on who will control of the Internet. Of course, only the United Nations can fill his prescription. TN Editor

Chinese President Xi Jinping on Wednesday called for greater cooperation among nations in developing and governing the internet, while reiterating the need to respect so-called "cyber sovereignty".

Speaking at an internet conference in Wuzhen, in the eastern province of Zhejiang, Xi and propaganda chief Liu Yunshan signaled a willingness to step up China's role in global internet governance, seeking to rectify "imbalances" in the way standards across cyberspace are set.

"The development of the internet knows no international boundaries. The sound use, development and governance of the internet thus calls for closer cooperation," Xi said in a video message at the start of China's third World Internet Conference.

While China's influence in global technology has grown, its ruling Communist Party led by Xi has presided over broader and more vigorous efforts to control, and often censor, the flow of information online.

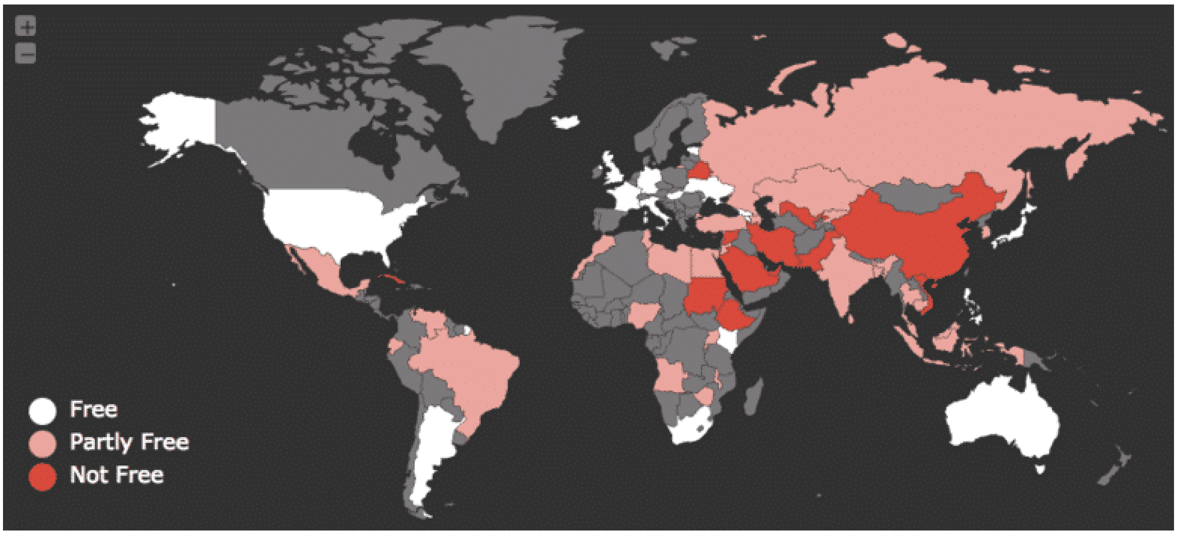
China infamously operates the so-called "Great Firewall", the world's most sophisticated online censorship system, to block and attack Internet services the government deems unsavory.

Xi repeated China's pledge to "promote equitable global internet governance" while upholding "cyber sovereignty", or the right of countries to determine how they want to manage the internet.

China's rubber stamp parliament adopted a controversial cybersecurity law this month that overseas critics say could shut foreign businesses out of various sectors in China.

More than 40 international groups and technology organizations have condemned the law, which introduces sweeping surveillance measures and local data storage requirements.

Read full article here…



Shock: Two-Thirds Of The World’s Internet Users Already Live Under Gov’t Censorship

The Internet is already heavily censored around the world by heavy-handed governments. Obama’s give-a-way of the Internet was thus not about censorship at all, but rather about the futuristic Internet of Things. ▯ TN Editor

Two-thirds of the world’s internet users live under regimes of government censorship, according to a report released today. The report from Freedom House, a pro-democracy think tank, finds that internet freedom across the globe declined for a sixth consecutive year in 2016, as governments cracked down on social media services and messaging apps.

The findings are based on an analysis of web freedom in 65 countries, covering 88 percent of the world’s online population. Freedom House ranked China as the worst abuser of internet freedom for the second consecutive year, followed by Syria and Iran. (The report does not include North Korea.) Online freedom in the US increased slightly over the year due to the USA Freedom Act, which limits the bulk collection of metadata carried out by the National Security Agency (NSA) and other intelligence agencies.

This year saw a notable crackdown on secure messaging apps such as WhatsApp and Telegram. WhatsApp was blocked or restricted in 12 countries over the course of the year — more than any other messaging app — including in Bahrain, Bangladesh, and Ethiopia, where authorities blocked it in response to civilian protests. Telegram faced restrictions in four countries including China, where the government blocked the encrypted messaging service due to its rising popularity among human rights lawyers.

“Although the blocking of these tools affects everyone, it has an especially harmful impact on human rights defenders, journalists, and marginalized communities who often depend on these apps to bypass government surveillance," Sanja Kelly, director and co-author of the *Freedom on the Net 2016* report, said in a statement Monday.

According to Freedom House, 24 governments blocked or restricted access to social media sites and communication services in 2016, compared with 15 last year. Internet freedom declined in 34 of the 65 countries included in the report, most significantly in Uganda, Bangladesh, Cambodia, Ecuador, and Libya. Both Brazil and Turkey had their rating downgraded to "partly free" and "not free," respectively, following high-profile web crackdowns in each country.

Read full story here…

China's 'Draconian' Cybersecurity Law Crushes

Free Speech

Technocracy in China has created a formidable barrier to protect itself: destroy free speech, the right to protest, the right to privacy. The Scientific Dictatorship is already calculating social scores on all citizens, using deep data mining technology, that will determine who to shun from societal benefits. Those who resist the 'Empire' will be stripped of anything that might make them a threat. □ TN Editor

China has today passed a controversial cybersecurity bill, tightening restrictions on online freedom of speech.

The bill also imposes new rules on online service providers, raising concerns it is further cloistering its heavily controlled internet.

The legislation, passed by China's largely rubber-stamp parliament and set to take effect in June 2017, is an 'objective need' of China as a major internet power, a parliament official said.

Amnesty International, however, said it was 'draconian' measure that violates people's rights to freedom of expression and privacy.

The ruling Communist Party oversees a vast censorship system, dubbed the Great Firewall, that aggressively blocks sites or snuffs out internet content and commentary on topics considered sensitive, such as Beijing's human rights record and criticism of the government.

It has aggressively blocked major companies such as Google and Facebook from offering their services in its domestic cyber space.

The law, which was approved by the National People's Congress Standing Committee, is largely focused on protecting the country's networks and private user information.

But it also bans internet users from publishing a wide variety of information, including anything that damages 'national honour', 'disturbs economic or social order' or is aimed at 'overthrowing the socialist system'.

A provision requiring companies to verify a user's identity effectively makes it illegal to go online anonymously.

Companies providing online services in the country must provide ‘technical support and help’ to public security organs investigating ‘crimes’, which would normally include those related to speech.

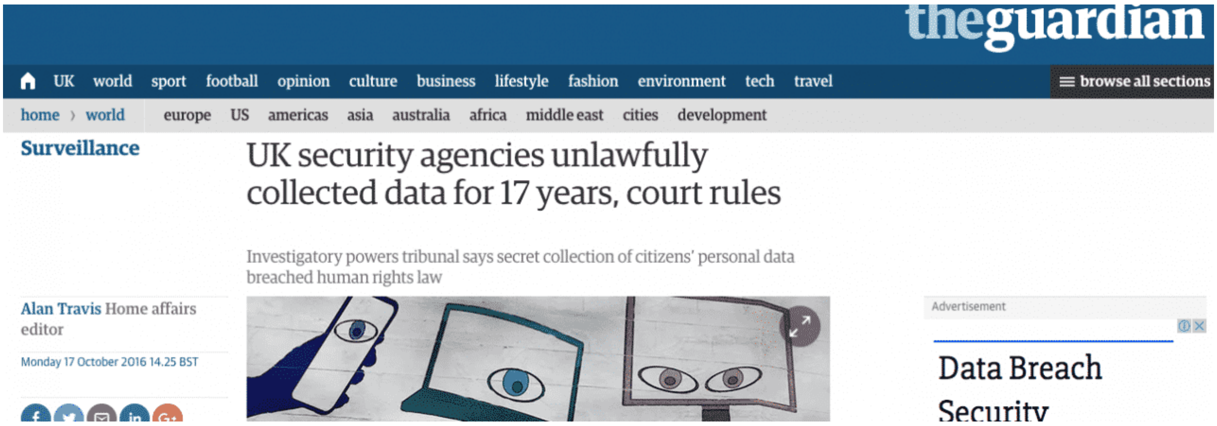
Read full story here…

Snowden Vindicated: Three New Scandals Show Pervasive Mass Surveillance

Mass surveillance is a global phenomenon, proving that the underlying thrust is for Technocracy, or Scientific Dictatorship. Every major country in the world is experiencing the same total surveillance mentality that we have in the U.S. TN Editor

While most eyes are focused on the presidential race between Hillary Clinton and Donald Trump, three major events prove how widespread, and dangerous, mass surveillance has become in the west. Standing alone, each event highlights exactly the severe threats which motivated Edward Snowden to blow his whistle; taken together, they constitute full-scale vindication of everything he's done.

Earlier this month, a special British court that rules on secret spying activities issued an emphatic denunciation of the nation's domestic mass surveillance programs. The court found that "British security agencies have secretly and unlawfully collected massive volumes of confidential personal data, including financial information, on citizens for more than a decade." Those agencies, the court found, "operated an illegal regime to collect vast amounts of communications data, tracking individual phone and web use and other confidential personal information, without adequate safeguards or supervision for 17 years."


theguardian
UK world sport football opinion culture business lifestyle fashion environment tech travel
≡ browse all sections
home › world
europe US americas asia australia africa middle east cities development
Advertisement
Data Breach
Security

Surveillance

UK security agencies unlawfully collected data for 17 years, court rules

Investigatory powers tribunal says secret collection of citizens' personal data breached human rights law

Alan Travis Home affairs editor

Monday 17 October 2016 14.25 BST

On Thursday, an even more scathing condemnation of mass surveillance was issued by the Federal Court of Canada. The ruling "faulted Canada's domestic spy agency for unlawfully retaining data and for not being truthful with judges who authorize its intelligence programs." Most remarkable was that these domestic, mass surveillance activities were not only illegal, but completely unknown to virtually the entire population in Canadian democracy, even though their scope has indescribable implications for core liberties: "the centre in question appears to be the Canadian Security Intelligence Service's equivalent of a crystal ball – a place where intelligence analysts attempt to deduce future threats by examining, and re-examining, volumes of data."

The third scandal also comes from Canada – a critical partner in the Five Eyes spying alliance along with the U.S. and UK – where law enforcement officials in Montreal are now defending "a highly controversial decision to spy on a La Presse columnist [Patrick Lagacé] by tracking his cellphone calls and texts and monitoring his whereabouts as part of a necessary internal police investigation." The targeted journalist, Lagacé, had enraged police officials by investigating their abusive conduct, and they then used surveillance technology to track his calls and movements to unearth the identity of his sources. Just as that scandal was exploding, it went, in the words of the Montreal Gazette, "from bad to worse" as the ensuing scrutiny revealed that police had actually "tracked the calls and movements of six journalists that year after news reports based on leaks revealed Michel Arsenault, then president of Quebec's largest labour federation, had his phone tapped."

Speaking this week at Montreal's McGill University, Snowden called for the resignation of Montreal's police chief and denounced the spying as a "radical attack on the operations of the free press." Canadian Prime Minister Justin Trudeau said "obviously I think that the troubling stories – troubling for all Canadians – coming out of Québec," adding: "we must and can continue to ensure protection of the press and their rights."

Read full story here…

Uproar In France Over Plan To Collecting Data On 60 Million Citizens

French citizens would do well to understand Technocracy and its incessant demand to collect data and more data, forever. There is never enough data to satisfy the urge to inventory and control. □ TN Editor

France’s government last week announced the creation of a highly controversial new database that will collect and store personal information on nearly everyone living in the country who holds a French identity card or passport.

The massive database, known as Secure Electronic Documents (Titres électroniques sécurisés or TES), was decreed by the government on October 30 in an effort to crack down on identity theft.

The move sparked immediate outrage in the French media, with weekly magazine L'Observateur describing it as "terrifying", and daily newspaper Libération calling it a "mega database that will do no good".

The TES will affect 60 million people and marks the first time the country has collected population data on such a scale since the start of the Nazi Occupation in 1940.

The database will include all the same information included on a French identity card or passport, depending on which a person holds: The first and last names, address, eye colour, weight, marital status, a photograph and the fingerprints of nearly everyone in France (with the exception of children under the age of 12) will be compiled into a single centralised system.

The information taken from passports will be stored for 15 years while identity card information will be kept for 20.

Same-same, but different?

French Interior Minister Bernard Cazeneuve was forced to defend the TES during a question-and-answer session in government on Wednesday following vocal criticisms of the system.

Justice Minister Jean-Jacques Urvoas also justified the database, saying it offered "better security for [identity cards and passports]" in a Facebook post published the same day.

Yet despite the efforts of Cazeneuve and Urvoas, both Socialists, it is unlikely that opposition to TES will dissipate. For some, the database signifies a renunciation of the values of the left. In 2012, former president Nicolas Sarkozy of the conservative Les Républicains party (formerly the UMP) proposed a similar system, which was slammed by the Socialists at the time.

"The two [databases] are relatively similar in the sense that the one proposed by Nicolas Sarkozy, which was known as the 'honest people's file', also sought to regroup all personal information linked to passports and identity cards, including digital photographs and fingerprints," Antoine Cheron, a lawyer specialised in emerging technologies with the

French firm ACBM, told FRANCE 24.

Ironically, one of the most vocal critics of Sarkozy’s “honest people’s file” was Urvoas, who has now been tasked with defending a similar system.

Read full story here…