MASTERING THE GENIE OF STATE SURVEILLANCE
(Lesson #4 from "Privacy, Surveillance, and Survival in America")

--Raj Balasubramanian
Raj@Solutioneer72.com

PART 1: The Problem

It was only in 2007, after about 8 years under total surveillance, when I finally received some vague confirmation that I was being targeted by the state, not just by non-state spooks and thugs for hire.

A colleague of mine at a Chicago public school pulled me aside, asked me why the police and the FBI were watching me from across the street, saw that I had no clue about what was happening, and then gave me a warm hug.

From that point onwards, I understood that, by extension, this meant my woman and my mother were also being targeted by state surveillance.

And I deduced that there was a state dimension behind the many surveillance modalities that were being used on us--from car / home / portable radio microphones, landline / cellphone wiretapping, and computer snoopware--to wireless hidden cameras, sneak-and-peek home intrusions, GPS vehicle tracking, and snail-mail monitoring--as well as the involvement of countless civilians.

Total state surveillance of this sort had been let out of the bottle once and for all by the USA PATRIOT Act of 2001 and its subsequent sunrise renewals, afterthought add-ons, and spreading spin-offs.

But, only as the smoke cleared little by little, were we able to make out more and more of this unleashed genie's robust powers.

FISA and CALEA

Already, from 1978, with FISA (Foreign Intelligence Surveillance Act), physical and electronic surveillance of so-called foreign agents was legalized under the supervision of a secret, rubber-stamp court, where only the state could be heard.

Operations on permanent residents and US citizens could proceed for up to 72 hours without a court order, while those on foreigners were given up to 1 year unsupervised. Probable cause eventually had to be shown regarding the target actually being an agent of a foreign power.

In 2001, 2004, and 2008, FISA was amended to cover non-state agents of terror and lone-wolf terrorists, as well

as to exempt surveillance of geographically-out-of-the-US targets from court oversight so long as analysts and their supervisors reasonably believed this one condition to be true.

From 1994, with CALEA (Communication Assistance for Law Enforcement Act), all telecoms and internet service providers (ISPs) were required to enable real-time access for warranted state surveillance of basic phone and internet interactions by building in these capabilities, with total non-detectability by targets as a key imperative.

In 2005, CALEA was upgraded to include VoIP and pending revisions aim to cover other emerging electronic communication technologies. But, in the meantime, it seems that the state has nevertheless leveraged extra-legal pressure on private-sector companies to obtain full access to peer-to-peer platforms such as Skype.

The USA PATRIOT Act and Its Offspring

Adding to these powers, The USA PATRIOT Act and its offspring authorized long-term state surveillance on all in America, including:

- warrantless access to internet activity, voicemail, library / phone / ISP / cable / other business records, and all 'tangible things';
- as well as court-warranted tactics, such as:
  - 'roving' wiretaps across multiple devices (with GPS tracking of cell phones),
  - sneak-and-peek physical searches with a 30-day deadline on after-the-fact notification (such 'black bag operations' are typically used to install spying devices and snoopware),
  - and GPS vehicle tracking--not to forget indefinite detentions, 'enhanced' interrogations, and renditions.

Targeting American citizens is permitted, if not solely based on actions protected by the First Amendment, and if related to foreign intelligence / espionage, (cyber)criminal activity, or terrorism.

Stellar Wind and Retroactive Immunity

From 2005 to the present, we have glimpsed at the genie's other, more secretive sides.

A year and a half too late to affect a pivotal presidential election, details about a covert NSA warrantless wiretapping program were finally released by a newspaper determined not to be scooped by its own reporter's upcoming book.

Supposedly targeting the non-US-origin communications of terrorists, Stellar Wind managed to somehow over-collect information from millions of non-terrorists actually in America, using spy rooms set up at key domestic telecommunication switchpoints.

Often justified as supposedly created in response to the 9/11 attacks, court documents reveal otherwise--that the program started in early 2001 itself.

But instead of applying FISA legal remedies--5 years of imprisonment or a $10,000 fine, $100/day in actual damages no less than $1,000, punitive damages, and court costs--for illegal surveillance, some cosmetic changes were made to the program description, laws were rewritten to allow what was previously barred, and total immunity was granted to all involved telecoms / ISPs by 2008.

Spying From Space

Perhaps state authorities would have taken a very different course of action if they had known that the NSA had also been targeting many among them--including a US Senate candidate currently serving as our President, a Senator aspiring to become our first female president, the Chair of the Senate Intelligence Committee, a 4-star General discredited by his marital infidelity, and all 9 Supreme Court judges--as recently disclosed by a former employee of a separate spy satellite division.

Mainway, Marina, Prism, Pinwale, Fairview, Blarney, Stormbrew, Oakstar, Nucleon...

Mainway and Marina

Now, in mid 2013, due to a classified document leak from a fugitive whistleblower, we have learned that, since the 2007 demise of Stellar Wind, the state has lawfully accessed all domestic and via-US-international telephony metadata without probable cause under another covert NSA program: Mainway.

Notwithstanding the centrality of telephony metadata to the purposeful spatiotemporal mapping of social networks, probable cause is said to be required in order to examine the contents of phone conversations--but it must only be presented before the secret, rubber-stamp FISA court, which has rejected literally just a handful of requests in 35 years under its non-adversarial, quasi-collaborative approach.

Regardless, according to one congressman, the NSA has admitted in secret briefings to allowing thousands of its agents to completely bypass this requirement under certain conditions--as proven true by subsequently released top-secret NSA / FISA documents.

And, as a complement to Mainway, the NSA uses its Marina program to similarly process the metadata of all internet communications, though some claim that these operations may have been suspended.

Prism and Pinwale

Thanks to the same fugitive whistleblower, we have also discovered that the state can lawfully access practically all real-time and archived internet communications from the servers of nine leading ISP / social media / web tech companies under the NSA's Prism program and process obtained image / video data through Pinwale.

People in the US are not supposed to be targeted, but with a 51% operating threshold for foreign-ness and a keen interest in those with foreign contacts, American citizens and permanent residents are sure to be ensnared.

Fairview, Blarney, Stormbrew, and Oakstar

Corporate denials about their involvement and statements parsing the technicalities of its extent are rendered moot by upstream data collection enabled by four other NSA programs: Fairview, Blarney, Stormbrew, and

Oakstar. Of these, Fairview seems to be tbe most all-encompassing, providing pure, pre-encryption access to covered communications.

Nucleon
And, as a complement, the NSA uses its Nucleon program to similarly process the contents of phone / VoIP conversations through speech-recognition capabilities.

Watching Your Ideas Form As You Type

With 84.19% of revelations still under wraps--in spite of the fugitive whistleblower's desire that this information be released in its entirety--the key journalist / civil liberties activist behind these leaks has promised that more will be exposed, probably after state authorities have exhausted their latest half-truths and revolving-door rationales.

While we wait, we do have something to ponder: a suggestive claim about the current power of state surveillance, from our fugitive whistleblower, who notes, "They quite literally can watch your ideas form as you type."

That is, it is no longer necessary to implant snoopware with a 'black bag operation', a niche-marketed trojan, or even a 'zero-day' exploit--the state already has instant access to all of our electronic communications.

If this is true--and the fact that our fugitive whistleblower has sacrificed a comfortable, $200,000-salary-a-year life in Hawaii with a very attractive female partner does attest to its truth--then the time for standing by and watching the genie take shape and grow in strength is definitely over.

But exactly what should we now do?

PART 2: The Solution

To preserve a dignified form of chaperoned, non-illusory privacy--along with sufficient existential security--We The People must transparently expose, collectively correct, and democratically master the genie of state surveillance, now forever out of its bottle.

Transparently Exposing the Genie

Transparent exposure means that all state-surveillance actions on American citizens and permanent residents must be declassified, shared with targeted individuals, and publicly released online--with certain exceptions for investigative and security concerns.

Omnisha:

- The state should consolidate the American targets of its various agencies, and fully detail actions taken on each target, in one permanent database: *Omnisha.*
- The state should provide each American target a hackproof mini-tablet for accessing their Omnisha file, searching out other targets by name or location, reciprocally sharing their files, and linking up with one another.
- The state should set up hackproof Omnisha terminals for established civil-liberties organizations such as the ACLU to facilitate their assistance of American targets with due process and constitutional protections.
- The state should enable Omnisha files to be instantly updated whenever any information about an American target is electronically entered by any agency and whenever the FISA court issues a ruling affecting that American target.
- Omnisha files must be non-deleteable, entries uneditable, and inputs logged.

A variegated cloak of secrecy:

- If the American target is a person of interest in an ongoing investigation, the state may electronically withhold information through Omnisha on any actions taken within 13 days prior to the current date. In other words, details of actions on a particular day would be automatically revealed to the target 13 days later.
- If the American target is a suspect in an attempted or committed violent crime, the state may extend this cloak of secrecy to 13 weeks back from the present. Details of actions on any day would be revealed to the target 13 weeks later.
- If the American target is a suspect in an attempted or committed terrorist act, the state may extend this cloak of secrecy to 13 months back from the present. Details for any specific day would be revealed to the target 13 months later.
- For non-American targets in the US (e.g., foreign visitors, tourists, students, guest workers, and undocumented persons), the state may extend this cloak of secrecy to 13 years back from the current date--unless the target's immigration status changes--and may exempt interim time the target spends outside the US.

Transparent exposure of this sort will open up information vital to ensuring that due process and other constitutional rights of American targets are properly respected.

Limiting the cloak of secrecy in this variegated manner will not only give the state enough time to effectively and efficiently investigate each target, but also it will help prevent frivolous, fear-driven witchhunts and long-term persecution.

The number 13 will remind us of our 13 colonies once under imperial oppression and therefore also of our eternal need for constitutional protections.

Collectively Correcting the Genie

Collective correction means that bad (provocational, abusive, biased) state surveillance must be replaced with good (preventive, benevolent, equitable) state surveillance, enforced by a People's Agency that surveils the state surveillors.

Preventive, Not Provocational

To be preventive, state surveillance must not be provocational.

- Targets--whether American citizens / permanent residents or just foreigners in the US--and the potential threats they pose must be de-escalated, not instigated.
  - Targets must be prevented from extremisizing towards committing any sort of harm, violence, or terrorism--not incited into extremist actions.
  - Targets must not be duped or encouraged in any way to commit any kind of harm, violence, or terrorism--particularly by undercover agents or proxies.
  - Targets must not be allowed to escalate towards committing any sort of harm, violence, or terrorism, because there is no guarantee that it can be safely contained.

- The state must aim to totally prevent harm, violence, and terrorism in the most peaceful, constructive, and appropriate manner--thereby neutralizing those who would do evil against us and routinely converting them to our American cause.

- Provoking targets towards committing harm, violence, or terrorism in order to set up a gotcha-style entrapment scheme is unacceptable, especially if done to simply score political points, get a spectacular arrest, or make a harsh example.

- Allowing targets to network and conspire with others towards committing harm, violence, or terrorism is unacceptable. Instead of cultivating evildoers, letting them plan evil together, smoking them out of hiding, and then seizing them up in sting operations, the state must shift its paradigm to one of total prevention.

- Last but not least, the state must not target any of us for just exercising our First-Amendment freedoms, including the freedom to take part in nonviolent, civil-disobedience actions that may break minor statutory laws or municipal codes. Such unjust targeting of activists is not only unconstitutional, but also--from a standpoint of preventing extremism--completely counterproductive. Instead of covertly infiltrating peaceful protest groups while still under a 13-day cloak of secrecy, state agents should overtly engage with such movement participants to further the common aim of preventing harm, violence, and terrorism.

Benevolent, Not Abusive

To be benevolent, state surveillance must not be abusive.

- No target should be physically, verbally, psychologically, or otherwise injured--or be caused pain--by the state, unless s/he is demonstrably escalating towards committing immediate or imminent harm, violence, or terrorism.

- No target should be intimidated, harassed, threatened, deceived, or otherwise mistreated by the state, unless s/he is demonstrably escalating towards committing immediate or imminent harm, violence, or terrorism.

- Instead of using any counterproductive tactics of abuse, the state must neutralize all threat potential from a target through honest, compassionate, constructive, and non-coercive engagement, unless s/he is escalating towards committing immediate or imminent harm, violence, or terrorism.

- This means the state must put all the cards on the table--from allegations and concerns to possible consequences and better outcomes--and then encourage the target to make the right and rewarded choices towards total harm reduction.

- By acting benevolently in this manner with the target, the state will not only be able to neutralize any danger s/he poses, but also be able to slowly overcome any extremist tendencies with the cultivation of self-actualizing behaviors.

- The state should provide neutralized targets with support from psychologists, social workers, and other care providers in the community--as well as minimum-wage employment and economic assistance, if necessary--to prevent recidivism.

Equitable, Not Biased

To be equitable, state surveillance must not be biased.

- The state should not engage in any racial, ethnic, religious, ideological, or other non-evidentiary forms of discriminatory (mis)profiling.

- This should be all the more so especially in the absence of any actual signs of unlawful, criminal, or threatening conduct.

Enforcing Good Surveillance

As decent human beings, we should be protected with good (preventive, benevolent, equitable) state surveillance, not persecuted by bad (provocational, abusive, biased) state surveillance (or rogue private-sector proxies, as previously discussed).

- The only way to ensure this is by surveilling the surveillors.
  - All law enforcement / state surveillance agents, buildings, areas, vehicles, and actions must be under total surveillance.
  - Individual employees must be required to wear either helmets or headbands fitted with a camera,

microphone, storage drive, and wireless transmitter.

- Interactions inside top-secret spyproofed meeting rooms should be totally recorded, unalterably stored, and specially accessible only on site.
- All of this meta-surveillance must be conducted with a 13-month cloak of secrecy so as not to obstruct the everyday operations of state authorities. In other words, state actions on any specific day will be automatically released for independent auditing 390 days later.

- PEGSSA (People's Enforcing Good State Surveillance Agency):
  - All audio / visual / textual / statistical / other meta-surveillance feeds will be reviewed after the 13-month cloak of secrecy by a new agency *PEGSSA*.
  - All Omnisha data will also be audited by PEGSSA as it becomes available following the expiration of individualized cloaks of secrecy.
  - After investigating meta-surveillance feeds for wrongdoing on the part of state authorities, PEGSSA will be empowered with the ability to file federal criminal charges on violators and required to publicize its findings online.
    - However, for meta-surveillance feeds concerning actions on foreigners in the US and state actions outside the US, PEGSSA charges and findings will be withheld under a 13-year cloak of secrecy starting from the action date.

- Compliance incentives and deterrents:
  - An unredacted, randomized compilation of ongoing processing by PEGSSA employees will be posted online daily for the public.
  - State agents found guilty of illegal or abusive surveillance must be punished under FISA guidelines on penalties for such actions (see above).

Democratically Mastering the Genie

Democratic mastery of state surveillance means holding it accountable and rightfully controlling it as a protective servant of We The People.

To effectively achieve this, we must transform America into a real democracy where the will of the people cannot be blocked by the forces of backwardness.

In a real democracy, the state will truly be of the people, by the people, and for the people--not of, by, and for the super-rich--nor of, by, and for corporations, banks and other institutions of a corrupt reigning bloc.

Unlike our current republican democracy, once America becomes a real democracy, every ableminded adult citizen will have a meaningful say and share in everything that matters to us.

And in that real democracy we will reach one day, We The People will look out for one another, take care of each other, and also set limits on one another.

As a crucial step in this direction, we need a direct-democracy constitutional amendment establishing a 4th popular branch of government with these powers:

- a People's Veto to overturn any federal, 'state', or local legislation;
- a People's Rule to create nationally-effective laws negating all contrary statutes;
- and a People's Recall to fire any elected or appointed official in our country, replacing that individual with the next in the relevant succession chain.

Any such Veto, Rule, or Recall would be absolutely binding, only if all of the following conditions are met during the election process of the proposed measure.

- At least 67% of the US voting-eligible population (based on data from the last presidential election) is registered to vote in the current election.
- At least 67% of these registered voters turn out to vote on the measure.
- And at least 67% of these actual voters vote in favor of the measure.

To qualify for a vote in a nationwide election held every 2 years on odd-numbered years, any proposed measure must meet these conditions in the prior year.

- At least 17.76% of registered US voters (based on data from the last presidential election) must petition the measure.
- The measure must not unanimously be held unconstitutional by the Supreme Court--something that would not be applicable for a Recall.
- And, for a Recall, the official must have completed 2 years in that position.

Structured so, this 4th popular branch of our government would significantly further integrate We The People into the American state--with the capability of decisively intervening to restore the popular will whenever that has been disrespected--while still leaving day-to-day operations under the care of the present 3 branches.

Empowered with these Veto, Rule, and Recall powers, We The People will be able to master the genie of state surveillance as we see fit, so that it can no longer do evil--neither in the light, nor from the shadows.

ADDENDUM: SLAYING THE MONSTER OF OVERSECRECY

Unnecessary, extreme secrecy is the Monster running amok in the castle of national security.

It is the Monster that has overthrown in spirit, if not in letter, a government that was meant to be of the People, by the People, and for the People.

If unstopped, this Monster will consume to the last drop all our civil liberties which are the vital lifeblood of our partial republican democracy.

To slay this Monster once and for all--speaking metaphorically for sustained nonviolent action by We The People--it must be dragged out into the bright light of day, subjected to the scorching sunshine that will scour away all its evil.

Therefore, as the first step in this countersurveillance manifesto, I have proposed programmatic transparency with compulsory disclosure as per a variegated cloak of secrecy.

In other words, all state surveillance actions must be logged in detail within a centralized database programmed to automatically capture such actions and alert targets (along with advocacy groups such as the ACLU, EFF, EPIC, and the National Lawyers Guild) immediately or up to no more than 13 months later, depending on where the targeted US citizen / permanent resident is listed on an innocence spectrum, from law-abiding American on one end to, on the other end, an American officially designated as a suspect in an attempted or committed act of terror.

Such programmatic transparency will empower ordinary Americans seeking due process and redress--while inevitably sparking revelation-based debates on the morality, constitutionality, legality, and basic decency of state surveillance practices.

Programmatic transparency, once enacted, will not only metaphorically slay the Monster, but also it will open the gates and lower the drawbridge for We The People to storm and seize the castle of national security--which is, after all, purpose-built for our protection, not our persecution.

As the rightful rulers of this castle, We The People will then be able to holistically reshape our national security agenda--away from counterproductive, neocolonial, imperialist tactics which only create ever-new monsters to endlessly menace us--and towards a geopolitics of cosmopolitan, eco-sustainable, and truly democratic global coexistence.