Krypt3ia

(Greek: κρυπτεία / krupteía, from κρυπτός / kruptós, “hidden, secret things”)

Enemy of the State

Fort Meade has acres of mainframe computers underground. You're talking on the phone and you use the word, "bomb," "president," "Allah," any of a hundred key words, the computer recognizes it, automatically records it, red flags it for analysis; that was twenty years ago.

> From The New Yorker; The Secret Sharer
>
> The government argues that Drake recklessly endangered the lives of American servicemen. “This is not an issue of benign documents,” William M. Welch II, the senior litigation counsel who is prosecuting the case, argued at a hearing in March, 2010. The N.S.A., he went on, collects “intelligence for the soldier in the field. So when individuals go out and they harm that ability, our intelligence goes dark and our soldier in the field gets harmed.”
>
> Top officials at the Justice Department describe such leak prosecutions as almost obligatory. Lanny Breuer, the Assistant Attorney General who supervises the department’s criminal division, told me, *“You don’t get to break the law and disclose classified information just because you want to.” He added, “Politics should play no role in it whatsoever.”*

Politics should play no role whatsoever? Really? This man is delusional to think that the statement, albeit correct, is actually factual. Of course politics play a part in such prosecutions, and case in point, this article cites examples of people getting slaps on the hand for breaking the espionage act and others where TS/S documents are concerned. The reasons that these others were not prosecuted to the full extent of the law was exactly because of politics and their entanglements. No Mr. Breuer, politics do play a role all too often.

That said, I encourage you all to read the full article and judge for yourselves just what happened with the case against Mr. Drake. It is my understanding from other sources as well as the New Yorker piece, that Drake was seeking to show waste on a grand scale while others were motivated by the idea that the sweeping changes to US law and oversight within the espionage area had taken a deep turn for the un-constitutional. This is an assessment that I agree with and have seen even more such dark turns lately where the digital realm is concerned. Frankly, at times I am a bit scared of the access and perhaps excess that the changes in the law have allowed for the NSA as well as anyone with enough juice within the newly minted security infrastructure post 9/11.

Constitutional Law vs. Technological Ease of Access vs. Political Agendas:

When the Constitution was created none of the technologies at play today were even a dream for the makers. Today though, the ideas of privacy, unreasonable search and seizure, and the fundamental freedoms we claim to cherish so much have been blurred. The blame for this rests partly on the technology, but mostly on the people who should be monitoring their system of laws. After 9/11 the people became all too trusting of the government to take care of them and all too willing to accept the over-reaches that they knew of while they were kept in the dark about others.

Case in point would be the FISA and warrantless wiretap situation that the Bush administration put into play after the terrorist attacks. It was the belief of the administration and the law enforcement community (certain factions) that too much time was lost to entering FISA warrants and getting approvals. So, instead they began to draft opinions that said the process was too ponderous, all the while they were putting together a secret process to just bypass the FISA altogether with or without the legal status to do so. This then begat the further access programs that essentially placed a tap on ALL communications going in and out of the backbone of the internet with the NARUS systems in the MAE's around the country.

Since the technology was there, and it could be placed into a position to audit everything, they just said let's do it. Thus, all traffic that you or I create over the Internet has the potential of being captured, flagged, and audited by someone at Ft. Meade without a warrant to do so. This also includes the cell phones as well because that traffic too passes through the same backbone system. Like the image of Brill above states;

> *Fort Meade has acres of mainframe computers underground. You're talking on the phone and you use the word, "bomb," "president," "Allah," any of a hundred key words, the computer recognizes it, automatically records it, red flags it for analysis; that was twenty years ago.*

Brill, a character from Enemy of the State, was going on about this in a film out before the attacks on the US. It would seem that if the technology had not already been in place then, the administration took a cue from the film and made it a reality after the twin towers came down. After all, the enemy could be anyone and the US populace wanted an action hero to take on the bad men and win. The same people though, did not seem to understand that to do so, the administration would take the shortcut of bypassing decades of laws set in place to protect our freedoms from excessive powers that the Bush administration wanted to have to 'protect' us.

It was this over-stepping of the laws that others within the story at The New Yorker had begun to tell to the Sun reporter and who now are being pursued by an alleged non political NSA and government for calling them on their breaking of the law. Just as much as Mr. Drake was seeking to show that the waste created by Trailblazer could also tie into the misuse of ThinThread's code to eavesdrop on anyone.

Both of these concerns are shared by me as well. After all, with the technology in place and without the oversight, how do we know that abuses aren't happening? The NSA is famously known to tell the Senate oversight committee to go pound sand… So, who is really watching the watchers?

Right Versus Wrong and Speaking Truth To Power; Do We Have A Say Anymore?:

So, if you have access to classified materials and programs and you see that things have gone off the rails how can you expect to report on it to the authorities and not be prosecuted? It used to be that there were protections, but, it seems now post 9/11 that changes to the paradigms of classification and the re-interpretation of the law to suit the state, it has become increasingly impossible to whistle blow and not be prosecuted. What's more, if you decide to report, the data that you are reporting on may be classified to the extent that it cannot even be used in open court or with your non cleared lawyer because it may be deemed too sensitive.

The net effect is that if there is malfeasance going on it may be impossible to report it and not get yourself into dire legal trouble with the current whistle blowing legislation on the books. This makes it even easier for the state and or entities and parties within its infrastructure to not abide by the law and have little to fear of oversight or speaking truth to power.

Sheeple vs. The Informed and Worried:

Meanwhile, the populace may live their lives unaware of the capacities for the state to listen to them and or present evidence gathered on them in an extra-legal way. At the very least, due to the wider interpretation of the law, it is easier for the state to gather and use evidence in ways that were not possible before because of the latitudes given post the Bush administration.

From a privacy perspective and the expectation thereof, the idea that all traffic is being hoovered up by the state is kind of scary. From a constitutional law perspective, you have the right to privacy in your papers and your domicile. Does this actually apply to digital papers, computers, hard drives, and anything you pass over telco lines to the cloud? Or is it considered public domain like your trash being placed at the end of your driveway?

This is an important precedent and should be considered with every email, IM, and call you make today. Just as well, if you are intent on retaining your privacy, what are the ways to do so now that all of these lines of communication are monitored by the state? One also has to determine just how worried they should be about intrusion into their privacy. After all, today we as a people give up a lot of information on ourselves at sites like Facebook and if we do that, just how much privacy can we expect?

Following that thought process, if we give up our privacy so easily how can we make an argument against the changes to the FISA rules as well as other laws where eavesdropping on our daily digital lives are concerned?

I for one do not want all of my conversations recorded for someone else to audit whether or not I may have said or done something that could be construed as illegal or perhaps pique the interests of the fed. Of course today one could easily be stopped in some states for alleged traffic violations and be asked if they could clone your phone data… Just because.

Whistle Blowing… Not So Much:

I guess in the end that the state of affairs today leans heavily toward the government being able to pretty much do what it wants to. From the warrantless wiretaps to the detention of non combatants, we have quite an inheritance from 9/11 and the Bush years. Unfortunately much of what President Obama had pledged he would roll back from those years have instead been re-approved if not enhanced. Add the whole Wikileaks debacle and now you have an even more reflexive and paranoid government trying to over classify everything and getting really bent when things get out.

So, the idea of whistle blowing I think is pretty much a dead one from here on. If anyone sees wrongdoing going on then they probably will let it go for fear that they will be prosecuted into oblivion.

And then the state wins… There have to be checks and balances.

K.

4 Votes

Ads by Google
Report SEC Violations
Whistleblowers in securities cases can recover up to 30%.
www.hbsslaw.com

About this entry

You're currently reading "Enemy of the State," an entry on Krypt3ia

Published:
May 24, 2011 / 10:44 pm

Category:
.gov, .mil, 1st Amendment, 4rth Amendment, A New Paradigm, Advanced Persistent Threat, Anonymous, Codes, COMINT, Commentary, Crypto, CyberSec, CyberWar, Digital Ecosystem, Dystopian Nightmares, Espionage, FBI, Geopolitics, History Repeats Itself, Honor, IMINT, INTEL

Tags:

---

1 Comment

Jump to comment form | comment rss [?] | trackback uri [?]