GlobalResearch
Center for Research on Globalization

Three Data Points Regarding Clinton's Email Server and the Law

By Washington's Blog
Global Research, June 09, 2016
Washington's Blog 3 June 2016

By Gaius Publius, a professional writer living on the West Coast of the United States and frequent contributor to DownWithTyranny, digby, Truthout, and Naked Capitalism. Follow him on Twitter @Gaius_Publius, Tumblr and Facebook. Originally published at at Down With Tyranny. GP article here

I've been writing for weeks that there are two aspects to the Clinton "secret server" issue — the way the server was handled, and the content of the messages it contained. Regarding the way the server was handled, almost everything needed to determine criminal liability is already in the public record and has been for a while.

So here are three data points, just three. They line up perfectly so the main idea is easy to grasp. (Consider this the first in a series, "The Clinton Server Story for Progressives." If events move too quickly, it will be the last, as everyone from *Time* to the *Washington Post* will be telling you what's what and you won't need me at all.)

- The server's email system was apparently unencrypted for the first two months of usewhen Clinton was Secretary of State.

This means that email going to and from the server was unencrypted during transmission. Messages were sent and received in plain text. This is the Washington Post from last March (my emphasis):

> The server was nothing remarkable, the kind of system often used by small businesses, according to people familiar with its configuration at the end of her tenure. It consisted of two off-the-shelf server computers. Both were equipped with antivirus software. They were linked by cable to a local Internet service provider. A firewall was used as protection against hackers.
>
> Few could have known it, but the email system operated in those first two months without the standard encryption generally used on the Internet to protect communication, according to an independent analysis that Venafi Inc., a cybersecurity firm that specializes in the encryption process, took upon itself to publish on its website after the scandal broke.
>
> Not until March 29, 2009 — two months after Clinton began using it — did the server receive a "digital certificate" that protected communication over the Internet through encryption, according to Venafi's analysis.
>
> It is unknown whether the system had some other way to encrypt the email traffic at the time. Without encryption — a process that scrambles communication for anyone without the correct key — email, attachments and

> passwords are transmitted in plain text.
>
> "That means that anyone could have accessed it. Anyone," Kevin Bocek, vice president of threat intelligence at Venafi, told The Post.
>
> The system had other features that made it vulnerable to talented hackers, including a software program that enabled users to log on directly from the World Wide Web.
>
> Four computer-security specialists interviewed by The Post said that such a system could be made reasonably secure but that it would need constant monitoring by people trained to look for irregularities in the server's logs.
>
> "For data of this sensitivity . . . we would need at a minimum a small team to do monitoring and hardening," said Jason Fossen, a computer-security specialist at the SANS Institute, which provides cybersecurity training around the world.
>
> The man Clinton has said maintained and monitored her server was Bryan Pagliano, who had worked as the technology chief for her political action committee and her presidential campaign. It is not clear whether he had any help. Pagliano had also provided computer services to the Clinton family. In 2008, he received more than $5,000 for that work, according to financial disclosure statements he filed with the government.

The Post article is much longer and contains a great deal of information. If this subject interests you, I encourage you to click through.

I hope you noticed the name "Bryan Pagliano" above. He's among the key people the FBI are talking to. In March, Pagliano was granted immunity in exchange for information. Pagliano is also the subject of a Judicial Watch FOIA request, and he's on the Judicial Watch deposition list. (For more on Pagliano, see below.)

Your first takeaway — Unless there was encryption employed by Clinton's private email service that no one knows about, email communications to and from it were readable as plain text. Certainly not deliberately so, but a fact nonetheless.

- The above-mentioned Bryan Pagliano has announced he's taking the fifth in his Judicial Watch deposition. He's going to refuse to speak when deposed.

The Hill:

> Clinton IT aide to plead Fifth in email case
>
> The man believed to have set up and maintained Hillary Clinton's private email serverwill assert his Fifth Amendment rights against self-incrimination and refuse to answer questions as part of an open records lawsuit against the State Department.
>
> Bryan Pagliano will decline to answer questions from Judicial Watch, the conservative legal watchdog group, during a deposition scheduled for Monday, his lawyers wrote in a court filing on Wednesday afternoon.
>
> The move forecloses the possibility that Pagliano would break his months of silence about the server issue, even as scrutiny has intensified on his role.

> Pagliano's lawyers told Judicial Watch more than a week ago that he would not be answering any questions, they claimed in their filing on Wednesday, and asked that it drop its subpoena. The organization refused.

"Taking the fifth" is an admission of guilt of *something* (who knows what?), but it's an absolute protection from prosecution by evidence from his own mouth. (The ability to "take the fifth," by the way, is important — it's our protection against evidence produced by torture. Still, it's damning, not just of Pagliano, but of that whole crew.)

Your second takeaway — Pagliano thinks he can be prosecuted for something if he speaks about the Clinton email server in his FOIA deposition. Check the first story above to review what he can speak about.

There will perhaps be political consequences from this. Will there be legal consequences? Keep reading.

- One of the laws that may have been broken is 18 U.S. Code § 793 – Gathering, transmitting or losing defense information.

Note first that the information listed below doesn't require a formal "classified" designation to be relevant, and second, that "intent" is not necessary to trigger the law's penalties. "Gross negligence" is sufficient. Again, my emphasis below:

> (f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information,relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer—
>
> Shall be fined under this title or imprisoned not more than ten years, or both.
>
> (g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

Your third takeaway — Unless this law doesn't apply for some other reason, it seems perfectly applicable for the reasons noted above. All sorts of State Department business and communications could be considered "relating to the national defense," including simple travel itineraries of top officials, such as President Obama's.

"Gross negligence" in allowing such documents to be "lost" or "stolen" is, under this law, a criminal act subject to fines, imprisonment, or both. If the server was hacked, broken into, the above law appears to apply.

Was This Law Actually Broken?

Were documents related to the national defense *in fact* stolen from Clinton's "home-brew"

server through negligence? I think that's the piece we don't know. Will we ever find out? That's the other piece we don't know. Still, these data points have been on my mind since I discovered them.

(By the way, the list of laws that may have been broken, not to mention State Department practices and guidelines ignored, is proffered to be long, at least according to the Internet. I've seen a list, and this is just one item on it. It's also the one I find least controvertible, since the meaning of "classified" is a mine field, depending on how each law is written, and this law isn't limited to "classified" material. I don't envy the FBI in sorting through all this.)

I'm not saying Clinton committed a crime; I'm not a lawyer, just a political observer. But as an observer, I do observe these data points, and suspect that they're related. And again, this is all from the public record, and every piece but the middle one has been there, out in the open, for a while.

Stay tuned. This may be nothing or not-nothing. But if it turns into something, you'll at least have heard about it.

Articles by: Washington's Blog