MEDIA BULLETIN
February 17, 2020
Garland Favorito

(404) 664-4044
garlandf@voterga.net
http://www.voterga.org

Trial Shows GBI, PAC Covered-up Gwinnett Security Flaws

LAWERENCEVILLE GA – The jury is out for the holiday weekend in the trial of Gwinnett Superior Court Judge Kathryn Schrader. **Trial evidence for the defense has painted an amazing picture of an obsolete, seriously flawed, and potentially compromised computer network that could not protect confidential judicial information of judges, clerks and staff** at the Gwinnett Justice Administration Center (GJAC).

Schrader and her staff discovered multiple network security breaches and repeatedly contacted Information Technology (IT) professionals from GJAC and Gwinnett County about exposures. Although they corrected some serious errors, **the IT staff was unable to identify a root cause of the network problems or implement a permanent solution**.

Schrader was first shocked to find **highly confidential Georgia Crime Investigation Center (GCIC) reports printed on her office multiple times** even though she should have no access to them**.** She later discovered **pictures and the personal passport of her son were exposed** to other GJAC employees**.** She also found **two Assistant District Attorneys were unauthorized "permissive users" on her computer**. Schrader then became concerned that the office of District Attorney (D.A.) Danny Porter had unauthorized access to her sensitive court documents.

Frustrated by security failures, Schrader, a self-described "forceps baby", sought help from Private Investigator T.J. Ward. Ward had former Forsyth Co. investigator Frank Karic connect a SharkTap **passive monitor** to her computer and retained forensics expert Ed Kramer to evaluate network packets. The SharkTap **duplicated packet data** going to and from Schrader's computer into a separate attached tablet for error detection. The tablet saved one set of PCAP files Kramer received in from the GJAC public guest network in an **encrypted, virtual private network** (VPN) to begin analyzing them for malicious attempts to penetrate Schrader's system.

Expert witness David Kalat explained the SharkTap approach was the **"best" way to monitor Schrader's computer.** His testimony confirmed assertions made last year by SharkTap creator Mark Chambers and VoterGA co-founders that SharkTap cannot remove network data and will not interfere with a network or alter its components. **No intelligible county data is transmitted externally**. Kalat explained how the PCAP files identified that **prior network malfunctions or hacking continually misdirected massive amounts of network traffic.** He determined either a network switch had "overflowed" **or the GJAC network was compromised by cyber-attack.** He also explained that **the SNMP protocol used by Gwinnett became obsolete in 1993.**

After Porter contacted the Georgia Bureau of Investigation (GBI), Schrader gave a notebook of details to cybersecurity agent Sara Lue**. But instead of trying to resolve the security failures, Lue assisted the Prosecuting Attorneys Council (PAC) with felony Computer Trespass charges against Schrader. Lue then submitted an affidavit to help Porter bring a false pornography charge against Kramer**. Lue and Porter claimed Kramer's computer had a picture that was actually a copyrighted photo by a renowned photographer from a web site Kramer accessed. Kramer's attorney filed a prosecutorial misconduct motion against Porter. That and other dubious 2019 charges filed by Porter against Kramer are now set for dismissal.