StopTheChamber.com

PO BOX 9576
Washington, D.C. 20016
info@velvetrevolution.us

February 23, 2011

Office of Bar Counsel
Board on Professional Responsibility
District of Columbia Court of Appeals
515 5th Street NW
Building A, Suite 117
Washington, DC 20001

Re: John W. Woods, Richard L. Wyatt Jr., and Robert T. Quackenboss

NOTICE OF COMPLAINT

I, Kevin Zeese Esquire, pursuant to Rule 8.3(b)—**Reporting Professional Misconduct**, on behalf of StopTheChamber.com and VelvetRevolution.us, NGOs dedicated to corporate and government transparency and accountability, herein lodge a disciplinary complaint against John W. Woods, Richard L. Wyatt Jr., and Robert T. Quackenboss, 1900 K Street, NW Washington, DC 20006. We ask the *Board on Professional Responsibility, District of Columbia Court of Appeals* to take immediate disciplinary action, including disbarment, against them for violations of the *D.C. Rules of Professional Conduct*.

SUMMARY OF THE COMPLAINT

John W. Woods, Richard L. Wyatt Jr., and Robert T. Quackenboss are members of the District of Columbia Bar and employed by the firm, Hunton & Williams ("H&W") in its Washington, D.C office. These lawyers, on behalf of their client, the United States Chamber of Commerce ("COC"), engaged, as the evidence below demonstrates, in an extended pattern of unethical behavior that included likely criminal conduct. Specifically, they solicited, conspired with and counseled three of its investigative private security firms to engage in domestic spying, fraud, forgery, extortion, cyber stalking, defamation, harassment, destruction of property, spear phishing, destruction of property, identity theft, computer scraping, cyber attacks, interference with business, civil rights violations, harassment, and theft.

In short, this unethical and criminal conduct involves "*dishonesty, fraud, deceit, or misrepresentation"* which violates the Rules of Professional Conduct, and undermines the rule of law, respect for the law and confidence in the law. Incredibly, as this conduct

occurred from November 2010 through February 2011, in dozens of calls, emails, proposals, meetings and conferences, none of the H&W lawyers ever expressed any reservation or doubt about the unethical conduct proposed and committed by their investigators. In fact, they actively solicited and approved everything that was proposed and presented. This, despite the fact that attorney John Woods had published an article in the February 2010 issue of *Data Protection Law and Policy*, titled "Social Networking and the e-Discovery Process," which stated that conduct such as that committed by the H&W investigators would "amount to misconduct under Rule 8.4 prohibiting 'dishonesty, fraud, deceit or misrepresentation." Exhibit A, p. 2.
http://www.velvetrevolution.us/images/H_WWoods_Social_Networking_Article.pdf

SPECIFIC VIOLATIONS

D.C. Rules of Professional Conduct Rule 8.4—**Misconduct**, states in pertinent part:
"It is professional misconduct for a lawyer to:
(a) Violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another;
(b) Commit a criminal act that reflects adversely on the lawyer's honesty, trustworthiness, or fitness as a lawyer in other respects;
(c) Engage in conduct involving dishonesty, fraud, deceit, or misrepresentation;
(d) Engage in conduct that seriously interferes with the administration of justice; …."

D.C. Bar Rule 1.2(e) states: "A lawyer shall not counsel a client to engage, or assist a client, in conduct that the lawyer knows is criminal or fraudulent." The scope of this rule is explained further: "a lawyer may not knowingly assist a client in criminal or fraudulent conduct. There is a critical distinction between presenting an analysis of legal aspects of questionable conduct and recommending the means by which a crime or fraud might be committed with impunity."

Attorneys John W. Woods, Richard L. Wyatt Jr., and Robert T. Quackenboss violated the above four provisions and counseled and assisted their client, the U.S. Chamber of Commerce, and their three private security contractor investigators, HBGary Inc, Palantir Technologies and Berico Technologies, to commit criminal and fraudulent conduct. It is well established that attorneys are accountable for the conduct of their investigators.

STATEMENT OF THE CASE

StopTheChamber/Velvet Revolution

StopTheChamber.com ("STC") is a campaign of VelvetRevolution.us ("VR"), a 501c(4) public charity since 2004 dedicated to corporate and government accountability. STC was launched in September 2009 in order to expose unethical activity, excesses and lack of transparency of the COC. STC urged companies and members to quit the COC to protest its potentially illegal tactics and strong-armed opposition to environmental

protection, financial reform, health care reform, worker safety and transparency. As a result, dozens of large companies and local Chambers of Commerce have quit the COC.

STC also sought out whistleblowers to provide inside information about the operations of the COC and its CEO Tom Donohue. STC received several tips, which it turned over to the FBI because the conduct disclosed involved allegations criminal activity inside the COC, including a three-page letter from a professed Chamber employee.

During the 2010 election campaign, STC exposed apparent violations of campaign finance law by COC, including reports of its use of illegal foreign money in elections, excessive compensation by CEO Donohue, misuse of tax-exempt status, money laundering, and use of the COC for the enrichment of its members. STC also reported on COC's partnering with American Crossroads to coordinate the spending of millions in secret money to support Republican candidates. The CEO of American Crossroads is former COC chief counsel, Steven Law. STC's sister organization, American Crossroads Watch, filed complaints against American Crossroads with the FEC, IRS and DOJ alleging violations of the Federal Election Campaign Act, and provided direct evidence of such violations to the FBI.

Chamber And Hunton & Williams Dirty Tricks Campaign Against STC/VR And Others

Over the past 18 months, the COC and its lawyers at H&W have responded to STC, not by having a debate in the public domain, but by intimidation and dirty tricks. When STC issued a press release about the COC in December 2009, COC/H&W responded by contacting FOX News, which wrote an article that resulted in STC being attacked with a coordinated campaign of more than 100 threats of violence, including death threats. Exhibit B. Once the FBI was advised of this threat campaign, the threats stopped. H&W also hired investigators to dig into the activities of STC and its principals, and provided disparaging and false information to reporters at FOX News, which FOX then published in various articles. On May 4, 2010, H&W lawyers a wrote letter to STC's Public Relations Agent Ilene Proctor repeating disparaging information about STC and one its principals. Exhibit C. On or about July 15, 2010, H&W wrote a letter to PR Newswire demanding that it remove a press release sent that week and disparaging STC. PR Newswire felt so threatened by the H&W letter that it scrubbed the press release from its Internet site.

In October 2010, H&W lawyers asked one of its investigator/contractors, Palantir Technologies, to help respond to a crisis facing another client, Bank of America, regarding a massive data leak to Wikileaks. On October 25, 2010, a Palantir employee, Matthew Steckman, wrote to H&W attorney John Woods ("Woods") that he would like to bring in two other private security companies, HBGary Federal and Berico Technologies to help with the project. *"Together, our three companies represent all facets of a complete intelligence and analysis capability. Ideally, we would like to set up a time to meet next week to brief you and Richard [H&W attorney Wyatt]…."* Exhibit D. The three companies formed a team called "Themis," named after the Greek God of law

and order. Themis created a "Corporate Information Reconnaissance Cell" proposal for H&W to present how it could target, track, and neutralize people, organizations, and companies as directed by H&W. Exhibit E. *"Team Themis is ideally suited to provide Hunton & Williams this critical capability…."* (page 2) *"Team Themis will provide full production and planning support throughout the entire targeting cycle in order to ensure that Hunton & Williams LLP has a clear, comprehensive understanding of the intelligence picture. We will work closely with the key leaders and decision-makers from Hunton & Williams to develop production requirements that meet their diverse needs."* (page 9) "*We will work closely with the key leaders from Hunton & Williams to determine key tasks and functions and ensure that we adjust our plan based on refined customer needs."* Id.

The techniques Themis described in the proposal were previously employed against the Colombian revolutionary organization FARC to track its rebels, and against violators of the trade ban with Iran as part of contracts with U.S. Government agencies, such as the Department of Defense and the FBI.

At a meeting in early November 2010, the H&W attorneys asked team Themis if it could use the same Themis techniques and technology against people and organizations opposed to another of its big clients, the COC. *See* Exhibits JJ and KK. Woods said later that it was the Palantir "Iranian shipping" presentation that "sold the Chamber." Exhibit Z. *See that presentation at* http://www.youtube.com/watch?v=iqMNzcspEyM Themis said that it could, and began preparing a massive $12 million plot to undermine STC, reporters Glenn Greenwald and Brad Friedman and others, including SEIU, Change to Win, Chamber Watch and Think Progress. Brad Friedman is also a principal of STC/VR.

On November 9, 2010, Woods wrote an email to HBGary CEO Aaron Barr ("Barr"), saying "*If you really want to impress Richard, I would look at the following web-site and tell him something about the guys behind it: http://velvetrevolution.us/stop_chamber/*" Exhibit F.

Later that day, Barr sent Woods an email: "*John, here is what I have found today. The real good stuff will come once we identify all these organization fronts and then start enumerating common players, influences, distributors, etc. Velvet revolution is a network of more than 120 progressive organizations…."* Exhibit G. The email goes on to list personal information about the principals of VR and their family members, promising to exploit "*pressure points*" of the named targets.

In another email that day, Barr wrote to Woods: "*Also I am already starting to collect information, associations on: [fixtheuschamber, US Chamber Watch Facebook pages, Stop The Chamber Facebook pages, stopthechamber and velvetrevolution]…."* Exhibit H.

Barr responded with information about targets SEIU, Change To Win and Chamber Watch, concluding with: "*I will focus on VR [Velvet Revolution]."* Exhibit I. In still another email that day, Barr told his partners: "*… I got a call from John while he was in*

the meeting with Richard at about 4:30 or so. We talked through some of the data, all went really well I think." Exhibit J. In that email thread, Woods told Pat Ryan from Berico that H&W had been gathering data about the Chamber opposition groups and would provide it on a data disc. "*Thanks for this, I am meeting on Tuesday with the team at HW who has gathered the underlying data.…"* Id.

On November 10, 2010, Woods wrote to Barr, "*I think we are good with Richard, let me work my end now. We may try to do a meeting with Richard on Friday – I will let you know shortly.…"* Exhibit K.

On November 11, 2010, Barr sent an email entitled "HW Meeting" with zip files of "*scraped Facebook*" pages from five NGOs and one principal of STC/VR. Exhibit LL. The email also included a six-page WORD document titled "Chamber Opposition," which listed information about NGOs, and personal information about principals and staff of STC/VR, including their friends and family. Exhibit MM.

On November 16, 2010, Barr wrote to his boss at HBGary, Greg Hoglund, about the contract with H&W. "*I have been sucked up for the last, seems like almost 2 weeks working the [H&W] law firm deal. The potential is huge for us. We are starting the pilot this week, 50K effort. After the pilot, the end customer [COC] gets briefed. We were talking to the senior partner of the law firm on Friday and he wants a firm fixed price by month for 6 months and the figure we have come to settle on is $2M per month for the 3 team members. That will equal $500-$700K for HBG Federal, that's (sic) per month."* Exhibit L.

In another email that day, Woods responded to Pat Ryan at Berico: "*Thank you. Please have Danielle work with Steve Patterson on the various documents.…"* Exhibit M. In that email thread, Ryan said: "*Hi John, Just wanted to send you a quick update as we follow-up from Fri's meeting. … The TA will include language to cover exclusivity related to any other corporate campaign projects. We are also putting together a brief amended proposal which will lay out tasks and deliverables for Phase I (initial analysis and products to support 23 Nov meeting with client) and Phase II (follow-on six months of enduring operations.…"* Id.

On November 23, 2010, Themis emailed each other about a conference call to *"discuss how the call with H&W should go?"* Exhibit N. In that email thread, Woods tells the team, *"Thank you for this. What I think would be very helpful is if we could set up a call later today of tomorrow where I could have my colleague Bob Quackenboss talk through with some folks on your team what tasks members of the team would actually be performing.…"* Id.

On November 29, 2010, Sam Kremin from Berico wrote to Barr: " … *Also, when I give these to Bob, I will emphasize that these are just examples to give to him an idea of what he is pitching to the Chamber and not at all indicative of our capabilities.…"* Exhibit O. In that email thread Barr proposes a dirty tricks campaign against the Chamber opposition organizations. Regarding Change to Win/ChamberWatch, Barr outlines the

"need to discredit the organization" by (1) "tying it to the unions," (2) "creating a false document and see if they pick it up," (3) creating "a fake insider persona and start communications with CtW. At the right point release the actual documents and paint this as an (sic) CtW contrived operation. They can't be trusted to stick to the truth, etc.," (4) connecting CtW "to velvet revolution and their radical tactics," (5) creating "two fake insider personas using one to discredit the other giving the second immediate legitimacy." Regarding VR, Barr says*, (1) "Attack [one of the VR principals] and after a series of attacks on his person start making ties to the back office folks … discrediting them by association. Done in the right way this can cause them to distance themselves and also funders from [the principal]." (2) "Attack their antics as self-serving and childish." (3) "[c]reate some [false] information and get them to run with it."* Id.

On December 1, 2010, Sam Kremin from Berico wrote to Woods and Quackenboss: *"John and Bob, Attached are the example reports that you request to give you a better idea of what we will be producing…."* Exhibit P. Attached to that email were four documents: (1) H&W Information Operations Recommendation with a list of dirty tricks to be used against Chamber opposition organizations, Exhibit Q; (2) H&W Organizational Assessment about Chamber Watch. Exhibit R; (3) Significant Activity Report about a "Protest near US Chamber of Commerce Building on October 7, 2010" Exhibit S; and (4) H&W Team Themis Slides, which is a series of eight color slides identifying the targets of Themis in a military/intelligence style presentation with different tiers and a "Priority Intelligence Requirement." Exhibit T.

On December 3, 2010, Palantir staffer Matthew Steckman wrote Woods: "*Updated with Strengths/Weaknesses and a spotlight on [reporter/lawyer] Glenn Greenwald…."* Exhibit U. In that email thread, Barr said: "*I think we need to highlight people like Glenn Greenwald. Glenn was critical in the Amazon to OVH transition and helped wikileaks provide access to information during the transition. It is this level of support we need to attack. These are established proffessionals (sic) that have a liberal bent, but ultimately most of them if pushed will choose professional preservation over cause, such is the mentality of most business professionals. Without the support of people like Glenn wikileaks would fold."* And Steckman wrote: "*Here is the collated first cut to brief John with at 9. I am going to send this to him at 8:15…."*

On December 10, 2010, Sam Kemin wrote Barr an email titled, "Ingesting FB Friends data," about scraping Facebook friends and placing that data in spreadsheets. Exhibit NN.

On January 14, 2011, Ted Vera from HBGary confirmed that H&W agreed to the Themis proposal "*50K to start – for a 30-day pilot project."* Exhibit V. In that email thread, Barr said; "*Lawfirm IO work is finally worked out…."* Sam Kremin said: "*Exciting news. We've received the data from H&W and it is a 189kb xml document. Ryan … could you integrate it into Palantir? Regarding the contract, Bob is really busy for the rest of this week, so we will meet to take care of that and receive his guidance and vision for the project sometime early next week. It would be great if we could get this data and the instance ready as soon as possible so we can start putting together products that will*

blow them away." Kremin also said: *"This afternoon an (sic) H&W courier is bringing over a CD with the data from H&W from phase 1. We are assuming that this means that phase 1 is a go…."* Id.

On January 19, 2011, Barr and HBGary staffer Mark Trynor discussed the "*scraping*" Facebook pages and data, including that of a principal of VR/STC. Exhibit W.

In another email that day, Barr, Trynor and Ted Vera discuss technical aspects of scraping VR's Facebook and social networking pages and specifically mention a VR principal's pre-teen daughter and the school she attends. Exhibit X.

On January 26, 2011, Woods emailed Barr about using Themis for a client working through another law firm, Booz Allen. Exhibit Y.

On February 3, 2011, Barr wrote to other Themis members that he had talked with Quackenboss "*ref our H&W support to the Chamber*…." He said that H&W wanted Themis to create a Phase 1 demo "*and then present jointly with H&W to the Chamber*…." Specifically, Barr suggested creating a "*5-10 min demo (along the lines of the Iranian shipping demo – which is what Bob Q said sold the Chamber in the first place….)… Bob apologized for the confusion/misunderstanding and said he thinks there is a high likelihood of selling the Chamber on this, but asked that we be willing to share the risk with H&W up-front. …. Please let me know where you … stand on this so I can get back to Bob ASAP and coordinate the next steps. …*" Exhibit Z.

The Themis Dirty Tricks Campaign Is Exposed

On February 4, 2011, Barr gave an interview to the *Financial Times* in which he stated that he had identified the leaders of the Anonymous network, a group of hackers that have supported Wikileaks and other freedom causes around the world. Barr indicated that he used techniques similar to those developed by Themis to gather this information. Exhibit AA. Joseph Menn, "Cyber Activists Warned Of Arrest*," Financial Times,* February 4, 2011 http://www.ft.com/cms/s/0/87dc140e-3099-11e0-9de3-00144feabdc0.html#axzz1EkOO41O2

In response, within two days, Anonymous seized control of HBGary's website, defaced its pages, extracted more than 70,000 company e-mails, deleted backup files, seized Barr's Twitter account, and took down the founder's website rootkit.com. It then posted all those emails in a searchable form on the Internet. Exhibit BB. "Anonymous Hackers Attack US Security Firm HBGary," *BBC Technology News,* February 7, 2011 http://www.bbc.co.uk/news/technology-12380987

The released emails created a frenzy of media coverage in major publications such as the *New York Times, Washington Post, LA Times, Forbes,* and *NPR*, in tech publications such as *Ars Technica, Wired, Tech News, The Tech Herald* and *The Hacker News*, in legal publications such as *Law Tech News, Corporate Counsel, Legal Times* and *National Law Journal,* and in independent media such as *Think Progress, The Brad Blog, Salon* and

FireDogLake. With each new revelation, reporters noted the breathtaking scope of the dirty tricks campaign, and the long list of crimes involved. Quotes from a few of the articles are set forth below.

- *"It proposed services to clients like a law firm working with Bank of America and the U.S. Chamber of Commerce that included cyber attacks and misinformation campaigns, phishing emails and fake social networking profiles, pressuring journalists and intimidating the financial donors to clients' enemies including WikiLeaks, unions and non-profits that opposed the Chamber."* Andy Greenberg, "HBGary Execs Run For Cover As Hacking Scandal Escalates," *Forbes,* February 15, 2011. Exhibit CC. http://blogs.forbes.com/andygreenberg/2011/02/15/hbgary-execs-run-for-cover-as-hacking-scandal-escalates/

- "*One of the files in those emails was a PowerPoint presentation that described 'the WikiLeaks Threat,' created by a group of three security firms that suggested Nixonesque tactics for sabotaging the site on behalf of Bank of America, including spreading misinformation, launching cyber attacks against the site, and pressuring journalists."* Andy Greenberg, "HBGary CEO Also Suggested Tracking, Intimidating WikiLeaks' Donors," *Forbes* Feb. 14 2011. Exhibit DD. http://blogs.forbes.com/andygreenberg/2011/02/14/hbgary-ceo-also-suggested-tracking-intimidating-wikileaks-donors/

- "*What is set forth in these proposals for Bank of America quite possibly constitutes serious crimes. Manufacturing and submitting fake documents with the intent they be published likely constitutes forgery and fraud. Threatening the careers of journalists and activists in order to force them to be silent is possibly extortion and, depending on the specific means to be used, constitutes other crimes as well. Attacking WikiLeaks' computer infrastructure in an attempt to compromise their sources undoubtedly violates numerous cyber laws."* Glenn Greenwald, "The Leaked Campaign to Attack WikiLeaks and Its Supporters," *Salon,* February 11, 2011. Exhibit EE. http://www.salon.com/news/opinion/glenn_greenwald/2011/02/11/campaigns

- *"For those new to the story, it involves email revelations that the U.S. Chamber of Commerce, the nation's largest corporate lobbying firm, was working with the law firm Hunton & Williams (H&W), to develop a scheme with three well-connected, government-contracted cyber-security/intelligence firms (HBGary Federal, Berico Technologies and Palantir Technologies --- calling themselves 'Team Themis' collectively) to use nefarious and likely illegal schemes in hopes of discrediting VR, myself and other progressive citizens, journalists and organizations who had opposed the Chamber's extremist corporate agenda."* Brad Friedman, "U.S. Chamber Plot Update: Malware, Fake Personas, Government Contracts, Public Shame, Bar Complaints, Media Failures and Other News," *The Brad Blog,* February 18, 2011 Exhibit FF. http://www.bradblog.com/?p=8363

- *"Last Thursday, ThinkProgress revealed that lawyers representing the U.S. Chamber of Commerce, one of the most powerful trade associations for large corporations like ExxonMobil and CitiGroup, had solicited a proposal from a set of military contractors to develop a surreptitious campaign to attack the Chamber's political opponents, including ThinkProgress, the Change to Win labor coalition, SEIU, StopTheChamber.com, MoveOn.org, U.S. Chamber Watch and others. The lawyers from the Chamber's longtime law firm Hunton and Williams had been compiling their own data set on some of these targets. However, the lawyers sought the military contractors for assistance.*

  As ThinkProgress has reported, the proposals — created by military contractors Palantir, Berico Technologies, and HBGary Federal, collectively known as 'Team Themis' — were discussed at length with the Chamber's lawyers over the course of several months starting in October of 2010. The core proposals called for snooping on the families of progressive activists, creating phony identities to penetrate progressive organizations, creating bots to 'scrape' social media for information, and submitting fake documents to Chamber opponents as a false flag trick to discredit progressive organizations." Lee Fang, "ChamberLeaks: Plan Solicited By Chamber Lawyers Included Malware Hacking Of Activist Computers," *Think Progress,* February 17, 2011. Exhibit GG. http://thinkprogress.org/2011/02/17/chamberleaks-malware-hacking/

VIOLATIONS OF D.C. RULES OF PROFESSIONAL CONDUCT

H&W lawyers, Richard Wyatt, John Woods and Robert Quackenboss, violated the D.C. Rules of Professional Conduct by counseling, assisting, advising, and conspiring with Themis to engage in unethical and criminal conduct on behalf of H&W client, the Chamber of Commerce. The evidence also shows that these lawyers, on behalf of Bank of America, violated the rules regarding their planned attack on Wikileaks, Anonymous and Glenn Greenwald, using similar dirty tricks. Although this complaint covers all these criminal violations as they relate to all the victims of this unethical dirty tricks plot, its main focus is on the conduct of the three H&W lawyers as it relates to STC and VR.

H&W lawyers knew of and participated in the following crimes and torts with Themis, and they never advised Themis to not to commit them. In fact, they did just the opposite by soliciting the conduct and conspiring to engage in the conduct. Many of these crimes are considered "Cyber Crimes," and are proscribed by a variety of federal statutes. The Department of Justice has published a manual called "Prosecuting Computer Crimes," listing a dozen statutes applicable to the likely crimes committed and planned by Themis and H&W. *See* http://www.justice.gov/criminal/cybercrime/ccmanual/ccmanual.pdf. The manual's appendix listing a litany of computer crimes is attached as Exhibit II. The crimes and torts committed by H&W/Themis include:

- **Creating forged documents**
- **Defamation**

- **Cyber stalking**
- **Spear phishing**
- **Violation of privacy**
- **Fraud**
- **Extortion**
- **Harassment**
- **Destruction of property**
- **Domestic spying**
- **Scraping of computer data**
- **Identity Theft**
- **Cyber attacks**
- **Interference with business**
- **Civil rights violations**
- **Conspiracy**

1. **Forgery and Fraud:** Themis planned to create forged documents with the intent that they be distributed and relied on by NGOs for the sole purpose of discrediting the NGOs and reporters. *See* Exhibits O, P, Q, T. Forgery and fraud are serious crimes under both federal and state law, and the same crime that resulted in the prosecution of Donald Segretti of Watergate infamy for forging documents to discredit Edmund Muskie.
2. **Defamation:** Themis planned to defame the reporters and principals of the NGOs, and quite possibly their families and staff in order to harm their reputation. *See* Exhibits O, P, Q, T. This constitutes an intentional tort under state law and is actionable in state and federal court.
3. **Cyber stalking and Harassment**: Themis not only planned but in fact began cyber stalking the principals, family, friends and members of the reporters and NGOs in order to intimidate them. *See* Exhibits H, P-U, FF. Cyber stalking, including when done anonymously, is a federal crime under both 18 U.S.C. § 875 and 47 U.S.C. § 223(h)(1)(C) and is a state crime in many jurisdictions. Other possible statutes violated are 47 U.S.C. § 223(a)(1)(C) (anonymously using a computer to threaten or harass a person); 18 U.S.C. § 2261A (using a computer in interstate commerce to engage in a course of conduct that places a person in fear of death or injury, including spouse and immediate family).
4. **Violation of Privacy**: Themis planned and did invade the privacy of reporters, and the principals of NGOs and their families and friends. *See* Exhibits W, X, MM. They scraped vast amounts of data from social networking sites -- in apparent violation of their Terms of Service -- identifying one principal's pre-teen daughter and the school she attends, another principal's "life partner" and sister, and then using that information to create reports on home addresses, dates of birth, and identifying staff of an NGO, including wives, sisters and children. Invasion of privacy is an intentional tort.
5. **Spear phishing:** Themis planned to spy on the computers belonging to NGOs and reporters through the implantation of illegal software programs that would open a

back door access to those computers. *See* Exhibit CC, GG. This is an illegal form of hacking prohibited by the federal Computer Fraud and Abuse Act, 18 U.S.C. **§** 1030.

6. **Extortion:** Themis planned to use extortionate tactics against reporter Glenn Greenwald and presumably others by uncovering information about weaknesses and using that information to "pressure" him, and others, to modify their positions or face ruin. *See* Exhibit O, U, GG. Extortion is a serious crime under both federal and state law. *See* e.g., 18 U.S.C. §§ 875–877, which prohibits using the mail to transmit in interstate commerce certain threats with the intent to extort, including threats to accuse of a crime or to injure person, property, or reputation. *See also*, 18 U.S.C. § 1030(A)(7) (transmitting and communication with intent a threat to cause damage).
7. **Destruction of Property and Cyber Attacks:** Themis planned to use viruses and malware to destroy the computers and data of NGOs and even engage in denial of service attacks against them. *See* Exhibits FF, GG. This violates 18 U.S.C. § 1030(a)(5)(A) (transmission of a program, information, code, or command, resulting in damage) as well as many state statutes.
8. **Theft, Identity Theft, and Internet Scraping:** Themis planned and in fact engaged in theft, identity theft, violation of the Digital Millennium Copyright Act, copyright infringement, and illegal scraping of NGO websites and social networking sites. *See* Exhibits H, O, W, X, FF, GG. This violates 17 U.S.C. § (DMCA), 17 U.S.C. § 506 and 18 U.S.C. § 2319 (criminal copyright infringement), 18 U.S.C. § 1028 (identity theft) and 18 U.S.C. § (wire fraud). Moreover, Facebook and LinkedIn specifically prohibit the use of software programs to harvest information from their sites. https://www.facebook.com/terms.php **("**You will not collect users' content or information, or otherwise access Facebook, using automated means such as harvesting bots, robots, spiders, or scrapers without our permission**.")** http://www.linkedin.com/static?key=user_agreement (prohibits "manual or automated software, devices, scripts robots, other means or processes to access, "scrape," "crawl" or "spider" any web pages or other services contained in the site" or to "[c]ollect, use or transfer any information, including but not limited to, personally identifiable information obtained from LinkedIn except as expressly permitted in this Agreement or as the owner of such information may expressly permit.").
9. **Spying and Interception of Electronic Communications:** Themis planned to use invasive cyber attacks to spy on NGOs and their staff and intercept electronic communications, and stored communications by accessing their personal and work computers. *See* Exhibits H, P-U, FF, CC, GG. This violates 18 U.S.C. § 2511 (intercepting electronic communications), 18 U.S.C. § 2701 (accessing stored communications), and 18 U.S.C. § 1030(a)(2) (accessing a computer and obtaining information).
10. **Interference with Business:** Themis planned to use deceptive means to ruin NGOs and undermine their funding. *See* Exhibit O, CC, DD, FF, GG. Interference with business and contracts is an intentional tort actionable in state and federal court.

11. **Civil Rights Violations:** H&W targeted NGOs and reporters for engaging in activities protected by the First Amendment, including the right to free speech, peaceful assembly, and petitioning the government for redress of grievances. *See* Exhibits O, CC, DD. Three private security contractors that received federal funding -Themis - were used by H&W to target the NGOs and reporters. Themis members used a portion of their federal funding to create the programs that were employed against NGOs and reporters. Themis used federal funding to create its Phase I pilot program for the COC, Bank of America and H&W. Because of this nexus to federal funds, Themis and H&W violated the civil rights of STC, VR and others as proscribed by 18 U.S.C. § 241 (conspiracy against rights) and § 242 (deprivation of rights under color of law).
12. **Conspiracy:** The lawyers of H&W conspired with members of the Themis team to violate all of the above statutes. Therefore, they are subject to prosecution under the general conspiracy statute, 18 U.S.C. § 371.

CONCLUSION

Richard Wyatt, John Woods, and Robert Quackenboss conspired with Themis to commit criminal acts, intentional torts and use "*dishonesty, fraud, deceit, or misrepresentation"* in their campaigns against STC/VR and others. In fact, the proposals they solicited and received discuss the use of "false documents," "fake personas," "false information," and using created "attacks" to "discredit" NGOs and reporters. Exhibits O and Q. Therefore, they are guilty of violating the D.C. Rules of Professional Misconduct. Incredibly, H&W attorney John Woods, a self professed expert in computer crimes, himself wrote just last year in an article entitled, "Social Networking Sites And The e-Discovery Process," http://www.velvetrevolution.us/images/H_WWoods_Social_Networking_Article.pdf that one type of conduct he engaged in with Themis constitutes a violation of Disciplinary Rule 8.4.

> *"Noting that lawyers are accountable for the behavior of their investigators, the Committee found that the 'friending' action proposed would amount to misconduct under Rule 8.4 prohibiting 'dishonesty, fraud, deceit or misrepresentation'. Therefore, 'friending' the witness on a social networking site without revealing that the purpose of the contact was to gain access to the restricted section of her profile constituted an act of 'deception' under the ethical rules. After reviewing the conflicting views of other State Bars on covert investigation by the legal profession, the Committee decided to refuse to acknowledge an exception as found in New York and other states ethics opinions and court decisions. Parties can also go too far when searching for 'evidence' on social networking sites. In the District of New Jersey case of Pietrylo v Hillstone Restaurant Group, a restaurant employee formed a by invitation-only discussion group called Spec-Tator on his MySpace page, intending it to be a space where other restaurant employees could negatively comment about their jobs. One member of Spec-Tator later provided uninvited members of the restaurant*

management with her access information. The management viewed the discussion group page and fired a number of employees as a result of information posted on Spec-Tator. Two of the terminated employees filed a lawsuit, claiming invasion of privacy.

Although the jury found that the plaintiffs did not have a reasonable expectation of privacy in the online group, the defendants were found to be in violation of the federal and state versions of the Stored Communications Act – 18 USC §§2701-11 and N.J.S.A2A:156A-27 - which make it an offense to access stored communications intentionally without authorization or in excess of authorization. The jury found that the employee who provided access to management had felt coerced, and so the access was not authorized. The jury subsequently awarded the plaintiffs $17,000 in compensatory and punitive damages." Exhibit A.

But, as detailed above, Woods and his colleagues at H&W engaged in conduct much more serious than mere deceitful Facebook friending. They engaged in criminal activity.

Reporter and attorney Glenn Greenwald excoriated H&W and attorney John Woods for their unethical conduct as detailed herein:

"But the real party here which deserves much more scrutiny is Hunton & Williams -- one of the most well-connected legal and lobbying firms in DC -- and its partner John Woods. Using teams of people scouring all the available emails, FDL has done its typically thorough job of setting forth all the key facts and the key players -- including from Booz Allen -- and Woods is at the center of all of it: the key cog acting on behalf of the Bank of America and the Chamber. It's Woods who is soliciting these firms to submit these proposals, pursuant to work for the Chamber and the Bank; according to Palantir emails, H&W was recommended to the Bank by the Justice Department to coordinate the anti-WikiLeaks work.

For a lawyer to be at the center of an odious and quite possibly illegal scheme to target progressive activists and their families, threaten the careers of journalists as a means of silencing them, and fabricate forged documents intended for public consumption -- and then steadfastly refuse to comment -- is just inexcusable. Perhaps some polite email and telephone encouragement from the public is needed for Woods to account for what he and his firm have done. In exchange for the privileges lawyers receive (including the exclusive right to furnish legal advice, represent others, and act as officers of the court), members of the Bar have particular ethical obligations to the public. At the very least, the spirit -- if not the letter -- of those obligations is being seriously breached by a lawyer who appears to be at the center of these kinds of pernicious, lawless plots and then refuses to account to the public for what he did." Glenn Greenwald, "More Facts Emerge About The Leaked Smear Campaigns," *Salon*, February 15, 2011. Exhibit HH.

http://www.salon.com/news/opinion/glenn_greenwald/2011/02/15/palantir

We urge the D.C. Board of Professional Responsibility to move quickly to discipline Richard Wyatt, John Woods and Robert Quackenboss for their unethical and criminal conduct in this matter. We strongly urge the Board to revoke the licenses of these attorneys.

Sincerely,

Kevin Zeese
Attorney at Law
301-996-6582