Spooky Business:
Corporate Espionage Against Nonprofit Organizations

By Gary Ruskin

Essential Information
P.O Box 19405
Washington, DC 20036
(202) 387-8030

November 20, 2013

TABLE OF CONTENTS

"The problem is that you do things in the service of your country that are just not appropriate to do in the private sector."[1]
-- John Brennan, director of the Central Intelligence Agency

Executive Summary

This report is an effort to document something we know little about: corporate espionage against nonprofit organizations. The entire subject is veiled in secrecy. In recent years, there have been few serious journalistic efforts – and no serious government efforts -- to come to terms with the reality of corporate spying against nonprofits.

Much of what we *do* know about this subject has been uncovered by accident. So the picture we have is fragmentary at best: just a few snapshots, taken mostly at random, arising from brilliant strokes of luck, giving a mere inkling of the full range of espionage activity against nonprofits.

There are, however, a few things we can say for certain.

The corporate capacity for espionage has skyrocketed in recent years. Most major companies now have a chief corporate security officer tasked with assessing and mitigating "threats" of all sorts – including from nonprofit organizations. And there is now a surfeit of private investigations firms willing and able to conduct sophisticated spying operations against nonprofits.

The use of former intelligence, military and law enforcement officers for corporate espionage appears to be commonplace. Especially prevalent is the use of former Central Intelligence Agency, National Security Agency and Secret Service agents, as well as current or former police officers, and other former military, intelligence and law enforcement officials. These current and former government employees, and current government contractors, do their spying against nonprofits with little regulation or oversight, and apparently with near impunity.

Many of the world's largest corporations and their trade associations -- including the U.S. Chamber of Commerce, Walmart, Monsanto, Bank of America, Dow Chemical, Kraft, Coca-Cola, Chevron, Burger King, McDonald's, Shell, BP, BAE, Sasol, Brown & Williamson and E.ON -- have been linked to espionage or planned espionage against nonprofit organizations, activists and whistleblowers.

[1] Eamon Javers, *Broker, Trader, Lawyer, Spy*. (New York: HarperCollins, 2010), p. xii. The quote is prior to Brennan's appointment as director of the CIA.

Many different types of nonprofits have been targeted with espionage, including environmental, anti-war, public interest, consumer, food safety, pesticide reform, nursing home reform, gun control, social justice, animal rights and arms control groups.

Corporations have been linked to a wide variety of espionage tactics. The most prevalent tactic appears to be infiltration by posing a volunteer or journalist, to obtain information from a nonprofit. But corporations have been linked to many other human, physical and electronic espionage tactics against nonprofits. Many of these tactics are either highly unethical or illegal.

Corporations engage in espionage against nonprofits with near impunity. Typically, they suffer nothing more than minor adverse media coverage if their espionage is exposed. The lack of accountability may encourage other corporations to conduct espionage.

Corporate espionage against nonprofit organizations presents a threat to democracy and to individual privacy. Democracy cannot function without an effective civil society. But civil society and its nonprofit organizations depend crucially on their ability to keep some ideas, information, and conversations private.

Individual citizens and groups do not lose their right to privacy merely because they disagree with the activities or ideas of a corporation. The right to privacy dovetails with our First Amendment rights to speech, public debate, and full participation in the "marketplace of ideas." It is especially unjust that corporations sabotage Americans' fundamental rights through actions that are unethical or illegal.

Many things can be done to protect nonprofits from corporate espionage. Congress should investigate and hold hearings on corporate espionage against nonprofits. Congress and state legislatures should enact legislation to criminalize the theft of confidential, noneconomic information held by their critics. Law enforcement – especially the U.S. Department of Justice – should prioritize investigating and prosecuting corporate espionage against nonprofits.

Introduction

The brave new world of corporate espionage

In the United States, corporations have hired private investigators since the colorful and enterprising Allan Pinkerton set up a detective agency in 1850. It was a benign start. Pinkerton enforced a strict code of ethics on his "private eyes," and he focused much of their work on solving crimes and catching criminals. But when Pinkerton died in 1884, his business was taken over by his sons, who had ideas of their own. They undertook controversial work, such as anti-union and strike-breaking operations. Thus began the long rise of the corporate spy-for-hire, and the effort to counteract those who dared to impair the profits of corporate America.

Today, most large corporations possess their own internal intelligence capabilities. There is an institutionalized security and intelligence function within every major company – a chief security officer of some sort. They perform "threat assessments" of all kinds, including the potential impact of nonprofit organizations.

Some of their staff or contractors are former employees of the National Security Agency, Central Intelligence Agency, Secret Service and other intelligence or law enforcement agencies, the military, or local police. Some of them have spent decades in intelligence work. A few giant corporations, such as Walmart, have essentially replicated in miniature an entire CIA directorate of intelligence – for their own private use.

Corporate espionage is now commonplace. Here's how the SANS Institute, a large cybersecurity education provider, explains it: "The increasing high stakes game of corporate espionage is being played by individuals, corporations and countries worldwide. These players will use any ethical, and in most cases, any unethical, means to acquire data that will give them a competitive or financial advantage over their competition."[2] Veteran reporter Eamon Javers makes a similar point. "There is so much money at stake," Javers says, "that everyone is spying on everybody else. We live in an information age where data is money. If you get more data than the next guy, you have the edge."[3]

Since the end of the Cold War, there has also been a large increase in the number of private investigative and intelligence firms – staffed with former government employees – doing espionage work largely unchecked by law enforcement. As Annie Machon, a former UK security agency MI5 agent, told the *New Statesman* "The big change in recent years has been the huge growth in these [security] companies….Where before it was a handful of private detective agencies, now there are hundreds of multinational security organizations, which operate with less regulation than the spooks themselves."[4]

---

[2] Shane W. Robinson, "Corporate Espionage 201." SANS Institute, 2007.
[3] Judith Woods, "Spies, Lies - and a Poisonous Divorce Battle." *The Daily Telegraph*, June 7, 2011.
[4] Stephen Armstrong, "The New Spies." *New Statesman*, August 11, 2008.

Eamon Javers has reported on the shady ethics of the corporate espionage industry. "As one experienced industry operative told me, 'We're just one scandal away from a government crackdown." With so much unsavory conduct taking place, the industry seems likely to explode into public view.

Former CIA division chief Melvin Goodman has similar concerns about these private intelligence firms. "Everything is being attracted to these private companies in terms of individuals and expertise and functions that were normally done by the intelligence community," he says. "My major concern is the lack of accountability, the lack of responsibility. The entire industry is essentially out of control. It's outrageous."[5]

Some of this lack of accountability and relative impunity may derive from cohesive "old boy networks" within former intelligence, law enforcement and military circles. Such camaraderie is not surprising. The CIA's "old boy network" is legendary. Regarding the FBI, Eamon Javers describes a little-known publication, the *Trapline*, which "lists every retired FBI agent in the country who works in the private investigations business." Javers describes the *Trapline* as "a bit like an institutionalized old-boy network for retired G-men."[6]

The rise of corporate espionage against nonprofit organizations

Throughout the twenty-first century, nonprofit organizations and activists have been targets of corporate espionage. But we don't know exactly how many. Little is publicly known about such espionage, because the perpetrators strive mightily to keep their operations secret. As one security journal observes, "most corporate espionage cases never come to light."[7] The entire subject remains murky at best.[8]

This report is an effort to document what we do know, even though the details in each case are far from complete. Much of what we know has been uncovered via improbable strokes of good fortune, such as whistleblowers within private investigations firms, leaked documents or bizarre coincidences. That suggests that what we do know is merely the proverbial tip of the iceberg.

Many factors have contributed to the rise of corporate espionage against nonprofits and whistleblowers, such as the rising availability of former CIA, NSA and other military,

---

[5] Jeremy Scahill, "Blackwater's Black Ops." *The Nation*, September 15, 2010.
[6] Eamon Javers, *Broker, Trader, Lawyer, Spy*. (New York: HarperCollins, 2010), pp. 112-3.
[7] "How Real Is the Risk of Corporate Espionage Today?" *Security Director's Report*, Institute of Management & Administration, April 2009.
[8] Two recent books are illuminating: Eveline Lubbers, *Secret Manoeuvres in the Dark: Corporate and Police Spying on Activists.* (London: Pluto Press, 2012); and Heidi Boghosian, *Spying on Democracy: Government Surveillance, Corporate Power and Public Resistance*. (San Francisco: City Lights Books, 2013).

intelligence and law enforcement officials; the outsourcing of government intelligence operations to private intelligence firms; the spread of surveillance techniques generally; the rising power and sophistication of electronic surveillance; the continued growth of corporate power in the United States; the paucity of law enforcement resources spent on protecting nonprofits; and the failure to punish corporations and their private intelligence firms for unethical or illegal espionage.

For many companies, the intangible value of their brand is a precious asset. For this reason, many companies may view nonprofits and whistleblowers as potent and unpredictable adversaries, and want to know everything they can about them. Companies take "brand risk" seriously, which also leads them to outsource their efforts to target nonprofit organizations, thus reducing the brand risk of such activities and hiding behind shields of plausible deniability.

Corporations have used a great variety of human, physical and electronic espionage tactics. According to Jack Devine, a 32-year veteran of the CIA, and former acting director of its foreign operations, "The private sector has virtually all the same techniques as the government."[9] Many of these techniques, at least when used by private corporations, are unethical or illegal, and have undeniably been used against nonprofit organizations.

A diverse array of nonprofits have been targeted by espionage, including environmental, anti-war, public interest, consumer, food safety, pesticide reform, nursing home reform, gun control, social justice, animal rights and arms control groups.

Many of the world's largest corporations and their trade associations -- including the U.S. Chamber of Commerce, Walmart, Monsanto, Bank of America, Dow Chemical, Kraft, Coca-Cola, Chevron, Burger King, McDonald's, Shell, BP, BAE, Sasol, Brown & Williamson and E.ON -- have been linked to espionage or planned espionage against nonprofit organizations, activists and whistleblowers.

Today, corporations can hire talented and experienced former intelligence, military and law enforcement officials to conduct espionage against nonprofit organizations. Former agents of the CIA, NSA, Secret Service, FBI, U.S. military and current and former police have all been linked to spying on nonprofits. The revolving door keeps spinning. Six years ago, the investigative reporter Douglas Frantz suggested, "The best estimate is that several hundred former intelligence agents now work in corporate espionage….These ex-spies apply a higher level of expertise, honed by government service, to the cruder tactics already practiced by private investigators."[10]

In recent years, there has been a large transfer of government intelligence operations from government staff to private firms. "The CIA, NSA and other agencies once renowned for their analysis of intelligence and for their technical prowess in covert operations, electronic surveillance and overhead reconnaissance have outsourced many of their core tasks to

[9] Douglas Frantz, "Spy. Vs. Spy." *Portfolio*, December 17, 2007.
[10] Douglas Frantz, "Spy. Vs. Spy." *Portfolio*, December 17, 2007.

private intelligence armies," writes Tim Shorrock. "As a result, spying has blossomed into a domestic market worth nearly $50 billion a year."[11] In 2010, the *Washington Post* was able to identify 1,931 private companies that "work on top-secret contracts." The *Post* also estimated that "out of 854,000 people with top-secret clearances, 265,000 are contractors."[12]

While such outsourcing is outside the scope of this report, it speaks to the immense capacity of intelligence gathering for hire, which corporations may employ to target nonprofit organizations.

In this report, we define corporate espionage as corporations' use of unethical or illegal investigative or surveillance techniques to obtain information about the activities of other corporations, whistleblowers, activists, and nonprofit organizations.

This report presents narratives of corporate espionage, most of them during the past seventeen years. We will also discuss some recent FBI investigations of nonprofit organizations, as well as a corporate-FBI partnership on intelligence matters.

[11] Tim Shorrock, *Spies for Hire: The Secret World of Intelligence Outsourcing*. (New York: Simon & Schuster, 2008), pp. 11-2.
[12] Dana Priest and William M. Arkin, "National Security Inc." *Washington Post*, July 20, 2010.

Narratives of corporate espionage

Beckett Brown International vs. many nonprofit groups

In 1994, John C. Dodd met Richard Beckett at a bar in Easton, Maryland. Shortly thereafter, Beckett introduced Dodd to Paul Rakowski, a retired Secret Service agent. Rakowski pitched to Dodd the idea of forming a new private security business. In August 1995, the private security firm Beckett Brown International (BBI) was formed.

As part of its work, BBI spied on many nonprofit organizations. James Ridgeway[13] of *Mother Jones*, who broke the story of BBI's espionage operations, wrote that BBI

> "spied on Greenpeace and other environmental organizations from the late 1990s through at least 2000, pilfering documents from trash bins, attempting to plant undercover operatives within groups, casing offices, collecting phone records of activists, and penetrating confidential meetings. According to company documents provided to *Mother Jones* by a former investor in the firm, this security outfit collected confidential internal records—donor lists, detailed financial statements, the Social Security numbers of staff members, strategy memos—from these organizations and produced intelligence reports for public relations firms and major corporations involved in environmental controversies."[14]

Greenpeace

For much of the 1990s, Greenpeace conducted a campaign to phase out the use of chlorine to manufacture plastics and paper. Especially in the early- and mid-1990s, Greenpeace's campaign generated critical media coverage for Dow, the world's largest producer of

[13] Incidentally, it was James Ridgeway who first reported in 1966 that private detectives (hired by General Motors, it was later disclosed) were tailing and investigating Ralph Nader. See James Ridgeway, "The Dick." *The New Republic*, March 12, 1966.
[14] James Ridgeway, "Black Ops, Green Groups." *Mother Jones*, April 11, 2008.

chlorine.[15] It also won support from the Clinton administration and other governmental bodies.[16]

In an effort to alleviate its political and publicity troubles, Dow hired Ketchum, a public relations firm. According to Mark Floegel of Greenpeace, Dow paid Ketchum roughly $500,000 annually for PR and espionage targeting Greenpeace and other environmental groups. Those operations included:

D-lines. BBI staff and contractors often conducted what they referred to as "D-lines," or obtaining Greenpeace's trash and recycling, to gain access to internal Greenpeace documents. According to a lawsuit filed by Greenpeace, between July 13, 1998 and July 18, 2000, BBI and its contractors conducted "more than 120 documented D-Lines at Greenpeace's offices."[17]

Mother Jones interviewed one participant in a D-line against Greenpeace:

> Jennifer Trapnell, who was dating [BBI employee Tim] Ward in the late 1990s, recalls an evening when she accompanied Ward on a job in Washington D.C. "He said they were trying to get some stuff on Greenpeace," she says. Ward wore black clothes and had told her to dress all in black, too: "It was *Mission Impossible*-like." In Washington, Ward parked his truck in an alley, she remembers, and told her to stay in the truck and keep a lookout. In the alley, he met a couple of other men, whose faces Trapnell did not see clearly. Ward was talking on a walkie-talkie with others, and they all walked off. About an hour later, the men came back and placed two trash bags in Ward's car. Trapnell says she didn't know what they did with the bags—and Ward never explained.[18]

---

[15] See, for example, Ivan Amato, "The Crusade Against Chlorine." *Science*, July 9, 1993. Elisabeth Kirschner and David Hunter, "Attacks on Chlorine Gather Force." *Chemical Week*, November 3, 1993. Margaret Kriz, "Clashing over Chlorine." *National Journal*, March 19, 1994. Bob Wyss, "Chlorine: Elementary, Perilous. Its Use in Compounds Trips International Research Alarms." *Providence Journal-Bulletin*, September 6, 1994. Ron Chepesiuk, "It's Chemical Warfare in Chlorine Battle; Greenpeace Wants a Global Ban on Chlorine, But Industry Groups Say There Is No Danger." *Orlando Sentinel*, April 9, 1995. Jim Morris, "In Strictest Confidence . . . The Chemical Industry's Secrets." *Houston Chronicle*, October 25, 1998.

[16] Brad Knickerbocker, "Clinton Would Bottle Up Use of Chlorine." Christian Science Monitor, February 22, 1994. "Panel Finds Threat to Great Lakes." *Associated Press/New York Times*, February 22, 1994.

[17] Greenpeace v. The Dow Chemical Company et al., at 9. See: http://www.greenpeace.org/usa/spygate/.

[18] James Ridgeway, "Black Ops, Green Groups." *Mother Jones*, April 11, 2008.

Use of police officers. To conduct D-lines against Greenpeace's Washington offices, BBI hired a subcontractor, James Daron, a District of Columbia police officer.[19] According to the Greenpeace complaint, Daron "was expected to use his official police badge to gain access to dumpsters that were enclosed by a locked fence." Daron participated in "at least 55" of the D-lines against Greenpeace.[20]

In an email discussing how to access the garbage and recycling of another nonprofit target, BBI's Tim Ward writes: "Maybe one of our BPD [Baltimore Police Department] guys can hit that one."[21]

Use of former Secret Service, CIA, military and police officers. BBI was founded and/or staffed by former Secret Service, CIA, military and police officers, including:

- David Bresett, former chief of counterterrorism for the Secret Service;
- Vincent Cannistraro, former director of counter-terrorism operations for the CIA;
- Philip Giraldi, former counter-terrorism specialist and military intelligence officer of the CIA;
- Jay A. Bly, former Secret Service agent;
- Timothy S. Ward, former sergeant, Maryland State Police;
- Paul Rakowski, former Secret Service agent;
- Michael Mika, former Secret Service agent;
- George M. Ferris, former naval special operations officer;[22] and,
- Harold "Jim" Grasman, former Secret Service agent, currently Special Agent in Charge and Chief Technology Officer, Office of Inspector General, US Department of Homeland Security.

Physical surveillance, intrusion and infiltration. According to the Greenpeace complaint, Mary Lou Sapone, a BBI consultant and experienced infiltrator of nonprofits, posed as a prospective campaign volunteer to surveil Greenpeace's offices. She reported that "I asked for a tour of all 4 floors in order to assess which divisions were largest, and observe all employees in their work space. The public affairs/public education/writing department was the largest in terms of floor space and number of employees observed."[23]

BBI apparently tried to determine the security codes for Greenpeace office doors, and may well have used these codes to enter Greenpeace offices. Found among the BBI documents related to Greenpeace was a handwritten list of security codes that seems to have been

---

[19] Daron still works for the District of Columbia police, in the special operations division. http://www.linkedin.com/pub/james-daron/2a/983/25.
[20] Greenpeace v. The Dow Chemical Company et al., at 9.
[21] James Ridgeway, "Black Ops, Green Groups." *Mother Jones*, April 11, 2008.
[22] James Ridgeway, "Black Ops, Green Groups." *Mother Jones*, April 11, 2008. BBI personnel chart and bios: http://www.greenpeace.org/usa/en/media-center/reports/BBI-personnel-chart/.
[23] Greenpeace v. The Dow Chemical Company et al., at 11.

used by BBI staff or contractors to try to open Greenpeace office doors. They apparently tested many codes, and noted which ones worked and which did not.[24]

According to the Greenpeace complaint, "BBI procured and held highly confidential Greenpeace records, including, for example, confidential personal, financial and employment records – which could only have been secured from Greenpeace's offices…"[25]

Wiretaps, hacking and other electronic surveillance. Ample evidence suggests that BBI and its sub-contractors conducted electronic surveillance of Greenpeace. According to the Greenpeace complaint:

- BBI kept a file labeled "Wire Tap Info" that was found along with Greenpeace internal documents.[26]

- "BBI hired TriWest Investigations to procure the phone call records of Greenpeace employees or contractors. BBI obtained the records of cellular phone calls placed and received by Greenpeace employees or contractors from Greenpeace's cellular provider. For example, BBI obtained a list of calls made to and from [Greenpeace organizer] Beth Zilbert's cell phone, which was paid for by Greenpeace."[27]

- "BBI purchased the services of NetSafe, Inc., a company that specializes in computer intrusion and electronic surveillance, for its work on Greenpeace projects. Most of NetSafe's top executives were former National Security Agency employees, including Joe Patanella." In 1999, BBI issued a $4,000 check, whose purpose was recorded as "Patanella – GP". "Other BBI records indicate that the check was issued for 'Cash' for 'Joe Patanella'."[28]

- BBI's notes to its clients "include *verbatim quotes* attributed to specific Greenpeace employees."[29]

- In 1999, BBI employees "wrote a proposal for 'intrusion and survey'" for Ketchum, which had been hired by Dow to work on matters related to Greenpeace.[30]

Theft of confidential information. According to the Greenpeace complaint, documents obtained from Greenpeace include "confidential strategy information" about Greenpeace's campaigns against "toxic chemicals, global warming, nuclear energy, genetic engineering

---

[24] http://motherjones.com/files/legacy/news/feature/2008/04/Handwritten-GP-Door-Codes.pdf. Greenpeace v. The Dow Chemical Company et al., at 13-14.
[25] Greenpeace v. The Dow Chemical Company et al., at 14.
[26] Greenpeace v. The Dow Chemical Company et al., at 14.
[27] Greenpeace v. The Dow Chemical Company et al., at 14-15.
[28] Greenpeace v. The Dow Chemical Company et al., at 15.
[29] Greenpeace v. The Dow Chemical Company et al., at 16.
[30] Greenpeace v. The Dow Chemical Company et al., at 16.

and the pollution of fisheries and oceans." Specific campaign strategy documents include: "Toxics Campaign Meeting Agenda for February 2, 1999; Genetically Modified Organisms Campaign Strategy; Global Warming Strategy; Climate Campaign Ship Tour Draft Schedule; Communications Plan for Great Bear Rain Forest Campaign; Greenpeace Southern Strategy Update; and Preservation of Whales Campaign."[31]

On November 29, 2010, Greenpeace filed a lawsuit in federal district court against Dow Chemical, Sasol North America, Dezenhall Resources, Ketchum and others regarding the corporate espionage. Greenpeace's complaint alleged violations of the Racketeer Influenced and Corrupt Organizations (RICO) Act including "both a pattern and practice of actions by the Defendants to intrude upon and invade the privacy and lawful interests of Greenpeace and misappropriate its confidential information for economic gain."[32] The suit was dismissed on September 9, 2011. Judge Rosemary M. Collyer ruled that "The direct victim of this alleged wire fraud was not Greenpeace**,** but a third party, and, therefore, the link between Greenpeace's injuries and Defendants' alleged racketeering activity is too attenuated to be actionable under RICO."[33]

On October 7, 2011, Greenpeace re-filed its lawsuit in District of Columbia Superior Court.[34] On February 5, 2013, DC Superior Court Judge Michael Rankin ruled that Greenpeace may proceed with parts of its case, but dismissed four of its claims.

On October 8, 2013, a coalition of nonprofit organizations filed an amicus brief in the District of Columbia Court of Appeals, urging the court to "declare the practice of 'commercial dumpster diving' to be an illegitimate means for a company to obtain information from an adversary." The brief defines "commercial dumpster diving" as "companies rummag[ing] through the trash of their competitors or critics in search of trade secrets or other valuable information."[35] The nonprofits filing the amicus brief include Essential Information; the Center for Health, Environment and Justice; Rainforest Action Network; Institute for Agriculture and Trade Policy; and the Center for Food Safety.

The Center for Food Safety, Friends of the Earth and GE Food Alert

In 2000, BBI changed its name to S2i. That same year, the public relations firm Ketchum asked S2i, on behalf of Kraft, to provide intelligence about nonprofit organizations opposed

---

[31] Greenpeace v. The Dow Chemical Company et al., at 17.
[32] Greenpeace v. The Dow Chemical Company et al., at 1-2. See also Spencer Hsu, "Greenpeace Accuses Dow Chemical, Sasol and P.R. Allies of Corporate Spying." *Washington Post*, October 29, 2010.
[33] Greenpeace, Inc. v. Dow Chem. Co., 808 F. Supp. 2d 262, 269. See also Tom Schoenberg, "Dow Chemical, Sasol Win Dismissal of Greenpeace Lawsuit." *Bloomberg*, September 9, 2011.
[34] For details, see: http://www.greenpeace.org/usa/en/news-and-blogs/news/spygate/.
[35] Greenpeace v. The Dow Chemical Company et al., amicus curiae brief from Essential Information et al., at 2-3.

to genetically engineered food. Emails related to S2i's operations suggest the company may have engaged in dumpster diving against these nonprofits and may have used a District of Columbia police officer to enter the premises of one of the nonprofits.

One document recovered from BBI's files was an email from Jay Bly, a former Secret Service agent, to Tim Ward, a former Maryland State Trooper:

> "Received a call from Ketchum yesterday afternoon re three sites in DC. It seems Taco Bell turned out some product made from bioengineered corn. The chemicals used on the corn have not been approved for human consumption. Hence Taco Bell produced potential glow-in-the-dark tacos. Taco Bell is owned by Kraft. The Ketchum Office, New York, has the ball. They suspect the initiative is being generated from one of three places:
> 1.Center for Food Safety, 7th & Penn SE
> 2.Friends of the Earth, 1025 Vermont Ave (Between K & L Streets)
> 3.GE Food Alert, 1200 18th St NW (18th & M)
> #1 is located on 3rd floor. Main entrance is key card. Alley is locked by iron gates. 7 dempsters [sic] in alley—take your pick.
> #2 is in the same building as Chile Embassy. Armed guard in lobby & cameras everywhere. There is a dumpster in the alley behind the building. Don't know if it is tied to bldg. or a neighborhood property. Cameras everywhere.
> #3 is doable but behind locked iron gates at rear of bldg."[36]

The next day, Bly sent Ward another email:

> "Re: Dumpster Dive.
> I got hold of Jim Daron [a District of Columbia police officer working for BBI] yesterday. He was supposed to do Vermont Ave and Penn Ave SE last night. I have not heard from him today—what's new. I did 18th St. Weard [sic] set up—the dumpster is behind locked gates. The truck drives down the alley and rings for the night guard to open the gate. The guard comes out, unlocks and goes back into the building (probably pissed off because they woke him up), the guys walk the bags out to the truck one at a time. When they finish they locked the gate behind them. There was so much trash they had to compact the truck two times while they were there. I did not find anything from the 5th floor, but the good news is it's doable."[37]

On September 28th, Ward replied:

> "Good news! Think that once Jim [Daron] calls you back we will know where we stand. If he can't get in with the shield, it will be difficult at sight #1. I think #2 we can do regardless. The issue is a hot one in general. I've been following it from here. Don't forget our GP [Greenpeace] boy in Baltimore has

[36] James Ridgeway, "Black Ops, Green Groups." *Mother Jones*, April 11, 2008.
[37] James Ridgeway, "Black Ops, Green Groups." *Mother Jones*, April 11, 2008.

been handling the work for GP. It may be worth a check in the city. Maybe one of our BPD [Baltimore Police Department] guys can hit that one."

U.S. Public Interest Research Group, Friends of the Earth, National Environmental Trust/GE Food Alert, Center for Food Safety, Environmental Media Services, Environmental Working Group, Institute for Global Communications, Pesticide Action Network.

One BBI document -- titled "Possible Sites" -- appears to be a list of nonprofit targets for dumpster diving, intrusion and infiltration. All of the groups above are on the target list. Next to Environmental Media Services is a notation: "think we have hit them before".[38]

Fenton Communications

Fenton Communications is a public relations firm founded by David Fenton that supports public interest, environmental and other nonprofit groups. *Mother Jones* reported that:

> On December 8, 1999, a BBI operative, according to an internal report, 'sat surveillance' at [David] Fenton's Washington home, beginning at 2:50 am. In the report, the operative noted the time of the morning garbage pick-up and that he returned to the office to 'sort material' and 'analyze.' BBI ran background checks on both Fenton and his then-wife. The company's files contained photographs of their house as well as client lists, billing information, and personnel information from Fenton Communications. Between July 1998 and February 2001, Fenton says, his firm experienced several break-ins, during which boxes of files and two laptops were stolen. The culprits were never caught.[39]

According to the Greenpeace complaint, BBI obtained confidential internal documents from Fenton Communications, including "billable time summary reports, reflecting the work performed for Fenton clients; internal fee memoranda, which provide instructions for invoicing particular clients; timeslip reports, which document the billable hours of each employee; and a check for the reimbursement of a health insurance claim for David Fenton, which was mailed to his home address."[40]

---

[38] http://motherjones.com/files/legacy/news/feature/2008/04/Possible Sites-Addresses.pdf.

[39] James Ridgeway, "Black Ops, Green Groups." Mother Jones, April 11, 2008. http://motherjones.com/files/legacy/news/feature/2008/04/Internal Report-Sat-Surveillance.pdf.

[40] Greenpeace v. The Dow Chemical Company et al., at 17.

Greenpeace, CLEAN and the Lake Charles Project

From 1984 to 2001, CONDEA Vista manufactured vinyl chloride at a factory in Lake Charles, Louisiana.[41] In 1997, CONDEA Vista was found guilty of "wanton and reckless disregard of public safety" and fined $7 million in punitive damages for leaks of ethylene dichloride, an intermediate compound in the production of polyvinyl chloride.[42] For many years Greenpeace campaigned to expose the dangers of polyvinyl chloride and the pollution generated by CONDEA Vista.[43]

According to the Greenpeace complaint:

- "On May 26, 1998, working at the behest of both CONDEA Vista and Dezenhall, BBI initiated the 'Lake Charles Project' to secure confidential information about environmental organizations and campaigners."[44]

- To assist with the Lake Charles Project, BBI hired Mary Lou Sapone, who hired Dick Rogers to infiltrate Greenpeace and CLEAN. "Posing as a concerned citizen, Rogers managed to get elected to CLEAN's board. From that position, he monitored the activities of Greenpeace, including communications between CLEAN and Greenpeace….Rogers sent more than 65 narrative reports and forwarded at least 150 confidential emails to Sapone. Sapone, in turn, forwarded the confidential emails and reports, almost daily, to Ward between August 1998 and November 1999."[45]

- "In 1998, Jay Bly traveled to Louisiana to surveil the offices and homes of activists working in Lake Charles. He submitted numerous reports detailing his activities, which involved…collecting and sorting trash from various locations. In 1999, Bly was reimbursed for supplies purchased in Maryland in connection with his CONDEA Vista investigations: AAA batteries, trash bags, a trash can and keys…the charge to CONDEA Vista for making 'keys' further provides support for the conclusion that BBI was unlawfully gaining access to Greenpeace premises, or property related to Greenpeace, that it had

---

[41] In 2001, CONDEA Vista was purchased by Sasol, a giant South African chemical company.
[42] "CONDEA Vista punished over leaks; CONDEA Vista Co. pays $7 million for chemical spill." *Chemistry and Industry*, November 3, 1997.
[43] See, for example, "Greenpeace, Lake Charles, La., Residents Protest PVC." Greenpeace news release, July 14, 1997. Jim Morris, "Bane On The Bayou; Chemical Companies' 'Lying Propaganda' Dupes The Public About Vinyl Industry Hazards, Lawmaker Says." *Houston Chronicle*, July 26, 1998. Gary Taylor, "Greenpeace Sets Louisiana Chem Protest." *Chemical News & Intelligence*, June 21, 1999. John McQuaid, "Unwelcome Neighbors: How The Poor Bear The Burdens Of America's Pollution." *Times-Picayune* (New Orleans, LA), May 23, 2000.
[44] Greenpeace v. The Dow Chemical Company et al., at 21.
[45] Greenpeace v. The Dow Chemical Company et al., at 23.

no lawful right to access."[46]

North Valley Coalition

According to *Mother Jones*,

"In 1996 and 1997 in northern California, where Browning-Ferris Industries was engaged in a battle over the future of a garbage dump, BBI conducted what its records labeled 'covert monitoring' and 'intelligence gathering' on the North Valley Coalition, a citizens group opposed to the Browning-Ferris project. In September 1997, BBI received a payment of $198,881.05 from BFI."[47]

Nursing home activists

According to the *Washington Post,* BBI spied on nursing home activists who wanted improved conditions at a Maryland nursing home called Hebrew Home:

> In 1997, at a community center in Montgomery County, activists held meetings to discuss Hebrew Home. The group, made up largely of residents' relatives, alleged poor medication controls and rough treatment of residents. As they strategized, an undercover operative was paying close attention. Her reports -- along with meeting agendas, license plate numbers and descriptions of advocates -- were relayed to Hebrew Home officials, the records show….Over a year, the nursing home paid BBI about $50,000 for investigative work, according to invoices addressed to chief executive Warren Slavin…[48]

Mary Lou Sapone and the Brady Campaign

From the mid-1990s through much of the 2000s, Mary McFate was a prominent volunteer for gun control groups. She ran for a seat on the board of directors of the Brady Campaign to Prevent Gun Violence, and worked closely with other national gun control organizations, such as the Violence Policy Center. She was director of federal legislation for States United to Prevent Gun Violence. She was deeply knowledgeable about the plans and actions of these and other national gun control groups. They, however, did not know that her other identity was Mary Lou Sapone, who since the late 1980s had been paid by corporations to

---

[46] Greenpeace v. The Dow Chemical Company et al., at 23-4.
[47] James Ridgeway, "Black Ops, Green Groups." *Mother Jones*, April 11, 2008.
[48] Jenna Johnson, "Corporate Espionage Detailed in Documents; Defunct Md. Agency Targeted Activists." *Washington Post*, June 22, 2008. See also Nathan Guttman, "Spying by Nursing Home Draws Fire." *The Jewish Daily Forward*, July 18, 2008.

spy on citizens' groups.[49] For example, she had worked for Beckett Brown International to infiltrate the Lake Charles, Louisiana environmental organization CLEAN.[50] For the U.S. Surgical Corporation, she had infiltrated animal rights activists who were protesting its use of dogs in medical training.[51] In a 2003 deposition, Tim Ward, former president of BBI, said that the National Rifle Association had been a client of Sapone's. Billing records show that the NRA paid BBI "nearly $80,000" for services rendered between May 1999 and April 2000.[52]

US Chamber of Commerce/HBGary Federal/Hunton & Williams vs. U.S. Chamber Watch/Public Citizen/Public Campaign/MoveOn.org/Velvet Revolution/Center for American Progress/Tides Foundation/Justice Through Music/Move to Amend/Ruckus Society

In January 2011, an executive in the computer security firm HBGary Federal claimed to have identified the leadership of the hacker collective Anonymous.[53] In response, the collective hacked the firm's email and other accounts, and released its files on the Internet.[54] This created a rare opportunity to review the recent internal workings of an important private investigative firm.[55]

The documents reveal proposals made by HBGary Federal to the powerful U.S. law firm Hunton & Williams, to help its client, the U.S. Chamber of Commerce, discredit its nonprofit critics.

The documents offer the joint services of three firms: HBGary Federal, the intelligence analysis firm Palantir Technologies[56] and Berico Technologies,[57] which provides

---

[49] James Ridgeway, Daniel Schulman and David Corn, "There's Something About Mary: Unmasking a Gun Lobby Mole." *Mother Jones*, July 30, 2008. John Stauber and Sheldon Rampton, *Toxic Sludge is Good For You: Lies, Damn Lies and the Public Relations Industry*. (Monroe, ME: Common Courage Press, 2002), pp. 61-4.
[50] James Ridgeway, "Black Ops, Green Groups." *Mother Jones*, April 11, 2008.
[51] Joseph Demma, Robert E. Kessler and Michael Slackman, "Bomb Suspect: 'I Was Set Up'; Says 'Friend' -- U.S. Surgical's Agent -- Persuaded Her to Go On." *Newsday*, January 27, 1989. Celestine Bohlen, "Animal-Rights Case: Terror or Entrapment?" *The New York Times*, March 3, 1989.
[52] James Ridgeway, Daniel Schulman and David Corn, "There's Something About Mary: Unmasking a Gun Lobby Mole." *Mother Jones*, July 30, 2008.
[53] Nate Anderson, "How One Man Tracked Down Anonymous—and Paid a Heavy Price." *Ars Technica*, February, 2011.
[54] Charles Arthur, "Anonymous Attacks US Security Company." *Guardian*, February 7, 2011.
[55] Eric Lipton and Charlie Savage, "Hackers' Clash With Security Firm Spotlights Inquiries to Discredit Rivals." *The New York Times*, February 12, 2011.
[56] For background, see: Pascal-Emmanuel Gobry, "Revealed: Palantir Technologies, The Secretive $735 Million Tech Security Company Helping Hedge Funds And Governments."

intelligence services to the U.S. military and intelligence agencies. Together, the three firms called themselves "Team Themis."

In response to solicitations from Hunton & Williams, several Team Themis documents outline a campaign to target U.S. Chamber Watch, a nonprofit watchdog group that monitored the U.S. Chamber of Commerce. Team Themis proposed to execute highly unethical and/or possibly illegal tactics,[58] such as:

- "Create a false document, perhaps highlighting periodical financial information, and monitor to see if US Chamber Watch acquires it. Afterward, present explicit evidence proving that such transactions never occurred."

- "[C]reate a fake insider persona and generate communications with CtW [Change to Win]. Afterward, release the actual documents at a specified time and explain the activity as a CtW contrived operation. Both instances will prove that US Chamber Watch cannot be trusted with information and/or tell the truth."[59]

Team Themis proposed to wage electronic warfare against U.S. Chamber Watch and its allies. One Team Themis proposal offers to employ HBGary Federal's capabilities for "Information Operations." Information Operations is a military term for electronic warfare. The proposal includes HBGary Federal's expertise in "Vulnerability Research/Exploit Development" and "Malware Analysis and Reverse Engineering."[60] Another Team Themis document proposes to use a software engineer "responsible for the design and development of custom bots".[61] Many kinds of malware use custom bots.

Other emails show that HBGary Federal investigated the critics of the U.S. Chamber of

---

Business Insider, March 10, 2011. Palantir Technologies has received $80 million in 130 federal contracts since 2009, including 50 contracts with the Department of Defense and 22 contracts with the Department of Justice, according to USASpending.gov (accessed October 28, 2013.)

[57] Berico Technologies has received $13 million in 91 federal contracts since 2008, including 52 contracts with the Department of Defense, according to USASpending.gov (accessed October 28, 2013.)

[58] See Kevin Zeese's ethics complaint against Hunton & Williams attorneys John W. Woods, Richard L. Wyatt and Robert T. Quackenboss, February 23, 2011. http://www.velvetrevolution.us/images/H_W_Bar_complaint.pdf.

[59] "US Chamber Watch Information Operations Recommendation." November 29, 2010. http://images2.americanprogress.org/ThinkProgress/ProposalForTheChamber.pdf.

[60] Berico Technologies, HBGary Federal, Palantir Technologies: "Corporate Information Reconnaissance Cell (CIRC); Team Themis." http://images2.americanprogress.org/ThinkProgress/themisproposal2.ppt.

[61] Berico Technologies, HBGary Federal, Palantir Technologies, "Corporate Information Reconnaissance Cell." November 3, 2010. http://images2.americanprogress.org/ThinkProgress/themisproposal1.pdf.

Commerce, including their spouses, children, religious activities and personal lives – and even gathered photos of them.[62]

Team Themis proposed to Hunton & Williams a $200,000 monthly price tag for initial research, with a $2 million monthly cost for a full campaign.[63]

Team Themis proposed to employ veterans of the U.S. military and intelligence services. In a proposal to Hunton & Williams, Team Themis wanted to "highlight…key personnel as representative of the outstanding talent within our organizations" who would conduct or oversee espionage against nonprofit organizations. Those people include:

- Guy Filippelli, "a former U.S. Army Military Intelligence officer with service in Germany, Korea, Iraq and Afghanistan, and as a civilian Special Assistant to the Director of the NSA….He most recently returned from several weeks in Afghanistan in June 2010, conducting a comprehensive assessment for senior defense and intelligence officials."

- Doug Philippone "deployed to Afghanistan, Iraq and Pakistan for a total of 6 deployments from 2003-2007. He commanded multiple Joint Special Operations Command outstations in support of the global war on terror. Doug ran the foreign fighter campaign on the Syrian border in 2005 to stop the flow of suicide bombers into Baghdad…. As a commander, Doug ran the entire intelligence cycle: identified high-level terrorists, planned missions to kill or capture them, led the missions personally, then exploited the intelligence and evidence gathered on target to defeat broader enemy networks."

- Aaron Barr, who "served as the Director of Technology for the Cyber security and SIGINT Business Unit within Northrop Grumman's Intelligence Systems Division….[He] served 12 years in the United States Navy as an enlisted cryptologist, senior signals analyst, software programmer, and system administrator….Mr. Barr has pioneered many uses of the Internet and new media for the purposes of conduction broad information operations campaigns for key intelligence customers."[64]

---

[62] Scott Keyes, "US Chamber's Lobbyists Solicited Firm to Investigate Opponents' Families, Children." Think Progress, February 10, 2011. Eric Lipton and Charlie Savage, "Hackers' Clash With Security Firm Spotlights Inquiries to Discredit Rivals." *The New York Times*, February 12, 2011.

[63] Berico Technologies, HBGary Federal, Palantir Technologies, "Corporate Information Reconnaissance Cell Scope of Work." November 15, 2010. http://images2.americanprogress.org/ThinkProgress/themisplan.pdf.

[64] Berico Technologies, HBGary Federal, Palantir Technologies, "Corporate Information Reconnaissance Cell." November 3, 2010. http://images2.americanprogress.org/ThinkProgress/themisproposal1.pdf.

Team Themis offered to infiltrate critics of the U.S. Chamber of Commerce. In a "brief" for Hunton & Williams, they propose to "use the following tactics to mitigate effect of adversarial groups." These tactics include: "Discredit, Confuse, Shame, Combat, Infiltrate, Fracture." They proposed using these tactics against the Center for American Progress, MoveOn.org, Velvet Revolution, Move to Amend, JTMP (Justice Through Music Project), U.S. Chamber Watch, Brad's Blog, Joe Trippi, Brave New Films, New Left Media, Agit-PoP, Courage Campaign and the Ruckus Society.[65]

Team Themis proposed to gather intelligence from several nonprofit organizations and their staff. One document sets forth some "priority intelligence requirements" and targets the following nonprofit organizations: MoveOn.org. Velvet Revolution, Center for American Progress, the Tides Foundation and Justice Through Music and U.S. Chamber Watch. Team Themis proposed to target these specific individuals: Brad Friedman, co-founder of the Velvet Revolution; Jane Johnson, a communications strategist; Ilyse Hogue, former director of political advocacy and communications for MoveOn.org; Nick Nyhart, president and CEO of Public Campaign; and Robert Weissman, president of Public Citizen.[66]

HBGary Federal/Hunton & Williams/Bank of America vs. WikiLeaks

In late November 2010, Julian Assange, editor-in-chief of the nonprofit media organization WikiLeaks, announced his intention to "take down" a top U.S. bank and reveal a corruption scandal within it. Bank of America was deeply concerned that it might be the subject of WikiLeaks' upcoming revelations.[67] HBGary Federal responded to these events with a joint proposal to Hunton & Williams – along with Palantir Technologies and Berico Technologies -- on how to destroy WikiLeaks. The proposal offers highly unethical and/or illegal tactics, including:

- Spread "disinformation" about WikiLeaks;
- "Submit fake documents and then call out the error." In other words, forging documents, giving them to WikiLeaks, and then exposing them as false, to undermine Wikileaks' credibility;
- Execute "[c]yber attacks against the [WikiLeaks] infrastructure to get data on document submitters". Palantir, HBGary and Berico believe that this would "kill" WikiLeaks.

---

[65] Berico Technologies, HBGary Federal, Palantir, "H&W Brief." http://thinkprogress.org/economy/2011/04/11/156819/chamberleaks-more-plans/.
[66] Team Themis, "Team Themis PIR's* [Priority Intelligence Requirements]." http://hbgary.anonleaks.ch/aaron_hbgary_com/attachments/1929.pptx.
[67] Nelson D. Schwartz, "Facing Threat From WikiLeaks, Bank Plays Defense." *The New York Times*, January 2, 2011.

- An implicit threat to ruin the career of Glenn Greenwald, a prominent journalist, if he continues to support WikiLeaks.[68]

In other documents presented to Hunton & Williams, for its client Bank of America, HBGary Federal boasts of its "IO [Information Operations] Mission Expertise." Information Operations is a military term for electronic warfare. HBGary Federal also offered its expertise in "Computer Network Attack", "Custom malware development", "Computer Network Exploitation", and "persistent software implants".[69]

The U.S. Department of Justice appears to have played a key role in these events. *The Tech Herald* reported that "Hunton and Williams were recommended to Bank of America's general counsel by the Department of Justice, according to the email chain viewed by The Tech Herald."[70] If this is true, it raises the question of whether the Justice Department assisted Bank of America in its battle against WikiLeaks, and how much Justice Department officials knew of and even supported corporate espionage against WikiLeaks and its allies.

Chevron/Kroll in Ecuador

In August 2010, a journalist named Mary Cuddehe wrote about the efforts by Kroll,[71] a giant private investigations firm, to recruit her as a "corporate spy" for Chevron. The company has been trying unsuccessfully to stave off a $9.5 billion fine arising from a lawsuit alleging that Texaco[72] spilled 330 million gallons of oil around Lago Agrio, Ecuador. The spill brought cancer and other diseases to local residents. According to Cuddehe, Kroll offered her $20,000 to pose as a journalist while conducting interviews to undermine a study of the health effects of the oil spill. She wrote, "If I went to Lago Agrio as myself and pretended to write a story, no one would suspect that the starry-eyed young American poking around was actually shilling for Chevron." Cuddehe turned down the money, and instead penned a charming article about her experience in *The Atlantic*.[73]

---

[68] "The WikiLeaks Threat: An Overview by Palantir Technologies, HBGary Federal and Berico Technologies." http://wikileaks.org/IMG/pdf/WikiLeaks_Response_v6.pdf.
[69] Nate Anderson, "Spy Games: Inside The Convoluted Plot To Bring Down WikiLeaks." *Ars Technica*, February 14, 2011.
[70] Steve Ragan, "Data Intelligence Firms Proposed a Systematic Attack Against WikiLeaks." *The Tech Herald*, February 9, 2011.
[71] Kroll identifies itself as "the leading global provider of risk solutions." See http://www.kroll.com/about/.
[72] In 2001, Chevron merged with Texaco.
[73] Mary Cuddehe, "A Spy in the Jungle." *The Atlantic*, August 2, 2010.

Walmart vs. Up Against the Wal

For years, Walmart has maintained a robust corporate intelligence and security department, staffed by a "team of former officials from the C.I.A., F.B.I. and Justice Department," according to the *New York Times*.[74]

In March 2007, Walmart's "Threat Research and Analysis Group" fired Bruce Gabbard, a computer technician, for unauthorized recording of conversations between Walmart and a *New York Times* reporter, Michael Barbaro, and intercepting Walmart colleagues' text messages. After leaving Walmart, Gabbard disclosed some of Walmart's surveillance practices, including targeting citizens groups and critics. According to the *Wall Street Journal*,

> "In late spring 2006, Wal-Mart learned that several anti-Wal-Mart groups might protest at the annual shareholders meeting in June. Company executives were concerned the civil-rights group Acorn (the Association of Community Organizations for Reform Now) and local Up Against the Wal members would disrupt its meeting. Wal-Mart sent a long-haired employee wearing a wireless microphone to Up Against the Wal's Fayetteville, Ark., gathering, and eavesdropped from nearby, says Gabbard. 'We followed around the perimeter with a surveillance van," he says.'"[75]

Électricité de France vs. Greenpeace

On November 10, 2011, the French utility Électricité de France was fined 1.5 million Euros for hacking into the computers of Greenpeace France. EDF was also required to pay an additional 500,000 Euros in damages to Greenpeace France. EDF hired the private intelligence firm Kargus Consultants, which in turn illegally obtained a copy of the hard drive of Yannick Jadot, the former campaign director of Greenpeace France. Thierry Lorho, the head of Kargus Consultants, was sentenced to three years in prison, two of which were suspended. EDF's former head of nuclear production security, Pascal Durieux, was also sentenced to three years in prison, with two suspended. His deputy, Pierre-Paul François, was sentenced to three years in prison, with 2½ years suspended.[76]

---

[74] Michael Barbaro, "Bare-Knuckle Enforcement for Wal-Mart's Rules." *The New York Times*, March 29, 2007. See also Jason Kirby, "When the Spies Are out of Control." *Macleans*, July 2, 2007.

[75] Ann Zimmerman, "Inside Wal-Mart's 'Threat Research' Operation." *The Wall Street Journal*, April 4, 2007.

[76] Henry Samuel Paris, "EDF Found Guilty of Spying on Greenpeace France." *Telegraph*, November 10, 2011. David Jolly, "Hacker, Cyclist, Executive, Spy." *New York Times* blogs, November 10, 2011. Hanna Gersmann, "EDF Fined €1.5m for Spying on Greenpeace." *Guardian*, November 10, 2011.

The story of the hacking and its discovery is magnificently convoluted. In 2009, a French investigating judge named Thomas Cassuto accidentally uncovered that Électricité de France had spied on Greenpeace France, and apparently other Greenpeace offices in Europe as well. EDF is the world largest operator of nuclear power plants. It is 85% owned by the French government. Greenpeace has long campaigned against the use of nuclear power.[77]

According to the *International Herald Tribune*, the French judge's investigation of a separate hacking operation was

> "picked up by a special cybercrime unit of the French Interior Ministry, [and] led to a French computer specialist, Alain Quiros…..As the French authorities delved more deeply into Mr. Quiros's computer, they found a copy of the hard drive of Yannick Jadot, the former campaign director of Greenpeace France, as well as that of Frédérik-Karel Canoy, a French lawyer and shareholder rights activist who has battled some of the country's largest companies, including Vivendi and European Aeronautic Defense & Space, the parent of the aircraft manufacturer Airbus….Mr. Lorho [a former French intelligence agent and head of Kargus Consultants] also admitted that he had collected data on Greenpeace. His client that time, he said, was Électricité de France, which had paid him for 'strategic intelligence' on anti-nuclear campaigners. Mr. Lorho has said his contacts at E.D.F. were 'perfectly aware' of the hacking and that such activities were understood to be included under the two one-year contracts he signed with the company….The investigation found that in addition to information on Greenpeace in France, E.D.F. obtained data on the environmental organization's activities in Spain, Belgium and Britain, where E.D.F. last year agreed to buy the largest nuclear power company there, British Energy…. In an interview with an intelligence Web site, Lerenseignement.com, Mr. Lorho said he assumed 'full responsibility' for hacking into the Greenpeace computer, but he added that ''I would like to see E.D.F., which sponsored the operation, take responsibility for its part.''[78]

There is evidence that EDF not only spied on Greenpeace France, but other Greenpeace offices in Europe. According to the *Guardian*,

> "A French investigation into allegations that France's state energy giant EDF spied on Greenpeace has taken a new turn after a suggestion in court documents that the company may have monitored environmentalists across Europe, including Britain….[The] French news website Mediapart, which has seen documents from the investigation, this week published extracts of the

---

[77] "Nuclear Conflict." *The Economist*, April 23, 2009.
[78] David Jolly, "Cycling Inquiry Exposes Corporate World of Spies and Hackers." The International Herald Tribune, August 1, 2009. See also Angelique Chrisafis, "Energy Boss Accused Of Spying On Greenpeace." Guardian, April 2, 2009.

> testimony by an EDF security executive and former police commander who is under investigation for conspiring to conduct illegal surveillance….Asked about a CD-rom of information from detectives that was found in his office safe, he said it contained information about environmental group structures and summaries of meetings. 'It was a question of the [Greenpeace] non-governmental group's organisation in Belgium, Spain, perhaps Britain, let's say Europe,' he added."[79]

E.ON/Scottish Resources Group/Scottish Power/Vericola/Rebecca Todd vs. the Camp for Climate Action

The Camp for Climate Action ("Climate Camp") is a climate activist group that started in the UK. It supports decommissioning of coal-fired power plants to mitigate carbon dioxide emissions that cause climate change. On October 17-18, 2009, approximately 1,000 activists from Climate Camp and other groups gathered to conduct civil disobedience to shut down the Ratcliffe-on-Soar coal plant.[80]

Sixteen months later, the *Guardian* reported that three large energy companies hired the private security firm Vericola to infiltrate the climate change activists.[81] The companies conducting the espionage were:

- E.ON, "one of the world's largest investor-owned power and gas companies. At facilities across Europe, Russia, and North America, our more than 72,000 employees generated approx. EUR132 billion in sales in 2012."[82] It is currently the world's 15th largest company.

- Scottish Resources Group, "the largest surface mining coal producer in the UK and the country's second largest coal mining company."[83]

- Scottish Power, a subsidiary of Iberdrola, a global Fortune 500 company and the 39th largest energy company in the world.[84]

---

[79] Angelique Chrisafis, "EDF Spied on Environmentalists in Britain, Court Documents Suggest." *Guardian*, April 17, 2009.
[80] Matt Ford, "The Eco Activists Who Are Camping Against Climate Change." CNN, October 20, 2009. Matt Dickinson and Danielle Dwyer, "Police Arrest 80 In Power Station Climate Protest." Press Association Mediapoint, October 18, 2009.
[81] Rob Evans and Paul Lewis, "Revealed: How Energy Firms Spy on Environmental Activists." *Guardian*, February 14, 2011. Paul Lewis and Rob Evans, "Special Report: Green Groups Targeted Polluters As Corporate Agents Hid In Their Ranks." *Guardian*, February 15, 2011.
[82] http://www.eon.com/en/about-us/profile.html
[83] http://www.scottishresources.com/About/SummaryInfo.aspx
[84] http://top250.platts.com/Top250Rankings/2012/Region/Industry

According to emails obtained by the *Guardian*, Vericola's chief executive, Rebecca Todd spied on activists by using "alias email addresses to express an interest in campaigns, subscribing to activist-only mailing lists…in July 2009, Todd said she was an activist…who wanted to make 'a positive contribution to the planet'."[85]

Burger King and Diplomatic Tactical Services vs. the Coalition of Immokalee Workers

The Coalition for Immokalee Workers is a community organization that advocates for the interests of low-wage immigrant workers in Florida. In 2008, CIW was conducting a campaign against Burger King, regarding the company's refusal to provide fair compensation to tomato pickers.

One day, CIW organizer Marc Rodrigues took a call from Cara Schaffer, who claimed she was a student at Broward Community College. She wanted to volunteer for CIW. But Rodrigues became suspicious when Schaffer asked about an upcoming conference call. When Rodrigues googled Schaffer, he found that she owns Diplomatic Tactical Services, "a security and investigative firm that advertises its ability to place 'operatives' in the ranks of target groups."[86]

Burger King has confirmed that it hired Diplomatic Tactical services "for years" and used it to obtain information about CIW's plans, and that "John Chidsey, the chief executive of Burger King, knew about the use of Diplomatic Tactical Services."[87]

The Pharmaceutical Research and Manufacturers Association and others vs. James Love/Knowledge Ecology International

James Love is the Director of Knowledge Ecology International, an organization that works to improve access to essential drugs, to reduce pharmaceutical drug prices worldwide, and to protect consumers in copyright. Love is an award-winning advocate; in 2006, KEI won a MacArthur Award for Creative and Effective Institutions, and in 2013, Love won a Pioneer Award from the Electronic Frontier Foundation.

On occasion, Love has been the target of corporate spying.

---

[85] Paul Lewis and Rob Evans, "Special Report: Green Groups Targeted Polluters As Corporate Agents Hid In Their Ranks." *Guardian*, February 15, 2011.
[86] Amy Bennett Williams, "Tomato Pickers Feeling Spied on; Aide Says Infiltrators Have Been at Meetings." *News-Press* (Fort-Myers, FL), April 12, 2008. See also Paul Demko, "Corporate Spooks: Private Security Contractors Infiltrate Social Justice Organizations." *Utne Reader*, January-February 2009.
[87] Eric Schlosser, "Burger With a Side of Spies." *The New York Times*, May 7, 2008.

Shortly after the passage of the Affordable Care Act, Love says he received a visit in his offices from a man who said he was recently let go from his job at Pharmaceutical Research and Manufacturers of America (PhRMA). "He said his job involved monitoring what I was doing, every day." Love said. "He told me that PhRMA had hired a private investigator to investigate us, from the West Coast." Separately, from 2007 to 2008, Love says that PhRMA and some companies in the copyright sector funded efforts to investigate the sources of funding for NGOs working on intellectual property issues, and to press those foundations to end their support of consumer advocacy.

Around 2008 or 2009, General Electric, Microsoft, Pfizer and other firms funded an effort by the National Foreign Trade Council (NFTC) to provide intelligence on NGOs working on intellectual property issues. Love says, "They approached someone we knew, with a proposal to provide information on Knowledge Ecology International and other NGOs working on intellectual property issues, as part of a program to counter NGO advocacy efforts on behalf of consumers." Eventually, Love says, the NFTC contracted with the Romulus Global Issues Management, an "international policy consultancy" that advises "several members of the Fortune 100."[88] The managing partner of Romulus is John Stubbs, whose wife is Victoria A. Espinel, a former Romulus employee. Espinel was U.S. Intellectual Property Enforcement Coordinator (IP czar) for the Obama administration, and is currently the CEO and President of the Business Software Alliance (BSA).[89]

Feld Entertainment vs. PETA, PAWS and other animal protection groups

People for the Ethical Treatment of Animals (PETA) has long opposed the exploitation of animals in the Ringling Brothers and Barnum & Bailey Circus. In 2002, PETA filed a lawsuit alleging that Kenneth Feld, chairman and CEO of Feld Entertainment Inc., had hired Clair E. George, a former CIA deputy director for operations, to surveil and disrupt PETA and other animal rights groups.[90] Feld Entertainment is the parent company of the circus. PETA's lawsuit was dismissed in 2006.

According to PETA, Feld's espionage operations were "run on a daily basis by a private eye named Richard Froemming…. From 1988 to 1998, Froemming and his several shell entities (with no employees or functions) were paid more than $8.8 million by Feld entities."[91]

The espionage operations succeeded in placing "approximately 16 undercover operatives at PETA, the Performing Animal Welfare Society (PAWS), the Elephant Alliance (EA), In Defense of Animals (IDA), and possibly other animal protection groups," according to PETA. These operatives "illegally recorded conversations in California and obtained highly confidential bank account numbers and bank information from Bank of America, credit

---

[88] http://www.goromulus.com/profile/
[89] Tony Romm, "Former White House IP adviser Victoria Espinel to lead BSA." *Politico*, August 28, 2013.
[90] "Rights Group Says Circus Spied on It." *The New York Times*, June 1, 2002.
[91] http://www.peta.org/features/ringling-bros-elephantgate.aspx.

card information, personal medical information, confidential internal financial records, and personnel information."[92]

In addition, both *Salon* and the *Washington Post* published long articles recounting the elaborate eight-year efforts of Kenneth Feld and Clair George to sidetrack a freelance reporter from writing about animal welfare scandals within the circus.[93]

BAE vs. Campaign Against the Arms Trade

In September 2003, the *Sunday Times* of London reported that BAE Systems[94] -- the world's biggest weapons firm[95] -- had hired a private intelligence-gathering firm to infiltrate activists opposed to the global arms trade.[96] According to the *Sunday Times*, BAE paid £120,000 per year "for at least four years" to a consultancy led by Evelyn Le Chene to infiltrate the Campaign Against Arms Trade. The group was infiltrated "by at least half a dozen agents in the 1990s." During this time, CAAT opposed the sale of BAE's Hawk jets to Indonesia. According to the *Sunday Times*, agents working for BAE

> "downloaded computer files, rifled through personal diaries, conducted surveillance on campaigners and passed on bank account details. Letters to and from senior Labour politicians including Jack Straw when he was home secretary, the MP Ann Clwyd and David Clark while he was the opposition spokesman on defence, were copied and sent to BAE. Meetings with MPs were reported on."[97]

BAE's espionage operations were effective, in part because BAE secured the services of "perhaps the most successful corporate spy of recent times, Martin Hogbin." According to the *Guardian*, "In 2003 security consultant Evelyn Le Chene was alleged to have been receiving emails from Hogbin, 58, who had spent six years rising through the CAAT. So successful was the alleged operation that Hogbin became a target for Met surveillance. Officers were convinced he was a key 'domestic extremist'."[98]

---

[92] http://www.peta.org/features/ringling-bros-elephantgate.aspx.
[93] Jeff Stein, "The Greatest Vendetta on Earth." *Salon*, August 30, 2001. Jeff Stein, "Send in the Clowns." *Salon*, August 31, 2001. Richard Leiby, "Send in the Clowns." *The Washington Post*, November 20, 2005.
[94] Until November 1999, BAE Systems was called British Aerospace.
[95] "SIPRI Rankings Say BAE World's Biggest Weapons Firm." *Agence France-Presse*, April 11, 2010.
[96] "Arms Firm Waged Dirty War On Protesters." *The Sunday Times*, September 28, 2003. See also George Monbiot, "The Parallel Universe Of BAE: Covert, Dangerous and Beyond the Rule of Law." *Guardian*, February 13, 2007.
[97] "Arms Firm Waged Dirty War On Protesters." *The Sunday Times*, September 28, 2003.
[98] Paul Lewis and Rob Evans, "Green Groups Targeted Polluters As Corporate Agents Hid In Their Ranks." *Guardian*, February 14, 2011.

In 2007, the Campaign Against the Arms Trade took legal action to force disclosure of the spying. It uncovered that Paul Mercer had been paid £2,500 per month by BAE's security department to spy on CAAT. According to the *Guardian*,

> "Mr. Mercer obtained a CD with details of confidential legal advice received from the peace campaigners' lawyers and at the end of last year passed it to Michael McGinty, head of BAE's security department….The litigation revealed that Mr. Mercer, who had a history of infiltrating peace groups such as CND [Campaign for Nuclear Disarmament], had disguised his dealings with BAE from his home in Loughborough….The Mercer operation came to light because BAE passed the information to its lawyers, Allen & Overy, who decided they had to disclose it to the court. BAE then fought to resist disclosure of their agent's identity."[99]

Global Open

Several news articles report that Global Open conducts espionage against nonprofit organizations. According to its website, Global Open (Europe) "advises our existing base of more than 90 clients"[100] and provides services such as intelligence gathering for "clients at a more serious level of threat from activism." Such services include, for example, a "24-hour warning service indicating, wherever possible, if a company is about to be targeted," and "[i]mmediate circulation of new activist tactics," and "[c]irculation of the movement of activist groups."[101] According to the *Guardian*,

> "The company best-known for monitoring protest groups is Global Open, founded a decade ago by Rod Leeming, a former special branch officer…[It] maintains 'a discreet watch' on protest groups that could damage a firm's reputation. It is understood to have offered to employ several ex-police officers, including [Mark] Kennedy, who said he was hired by Leeming last year….Court documents reveal Global Open to be one of two companies involved in the monitoring of the Campaign Against the Arms Trade for arms manufacturer BAE."[102]

---

[99] Rob Evans and David Leigh, "BAE Spy Named By Campaigners Is Friend Of Leading Tory." *Guardian*, April 19, 2007. See also Mark Thomas, "Martin and Me." *Guardian*, December 4, 2007.

[100] http://www.globalopen-uk.com/about_us/

[101] http://www.globalopen-uk.com/services/

[102] Paul Lewis and Rob Evans, "Special Report: Green Groups Targeted Polluters As Corporate Agents Hid In Their Ranks." *Guardian*, February 15, 2011. See also Rob Evans, Amelia Hill, Paul Lewis and Patrick Kingsley, "Mark Kennedy: Secret Policeman's Sideline as Corporate Spy." *Guardian*, January 13, 2011.

Inkerman Group and C2i vs. Plane Stupid

According to the *Guardian*, another company that conducts "monitoring [of] protesters" is the Inkerman Group. According to its website, the Inkerman Group is an "international business risk and intelligence company."[103] The Guardian reports that the Inkerman Group

> "employs former Met commissioner Lord Imbert as a strategic adviser. A 'restricted' report produced by the company three years ago warns of a growing threat of 'eco-terrorism'. Under a section on 'recent acts of eco-terrorism', the document lists a number of peaceful campaign groups, including the anti-aviation collective Plane Stupid. Some of those named in the Inkerman document were in fact spied on by Toby Kendall, who worked for another security firm, C2i International. He posed as 'Ken Tobias' in an attempt to infiltrate the anti-aviation collective Plane Stupid. Activists became suspicious of him as he appeared so eager to take part in direct action. His true identity was discovered on a social networking website, Bebo…. C2i has said Kendall was operating on his own."[104]

Brown & Williamson/Investigative Group vs. Jeffrey Wigand

In 1993, Jeffrey Wigand was fired by the tobacco company Brown & Williamson Tobacco Corp. He later became perhaps the most important tobacco industry whistleblower ever. Wigand made a number of high-profile allegations against the company, including that B&W Chairman Thomas Sandefur lied to Congress under oath about nicotine addiction.

According to the *Wall Street Journal*, B&W responded by hiring a "formidable team" of lawyers and private detectives to investigate and discredit him, including:

> "lawyers from the big New York firm Chadbourne & Parke and Atlanta's King & Spalding, and top New York public-relations adviser John Scanlon. They are working with the Investigative Group Inc., a leading Washington-based detective firm whose New York office is run by a former [and current] New York City police commissioner, Raymond Kelly. This is the firm Ivana Trump hired to investigate her rival Marla Maples and that Sen. Edward Kennedy used to check into an opponent in his 1994 campaign."[105]

---

[103] http://www.inkerman.com/gb/home.

[104] Paul Lewis and Rob Evans, "Special Report: Green Groups Targeted Polluters As Corporate Agents Hid In Their Ranks." *Guardian*, February 15, 2011.

[105] Suein L. Hwang and Milo Geyelin, "Getting Personal: Brown & Williamson Has 500-Page Dossier Attacking Chief Critic --- Court Files, Private Letters, Even a Suspicious Flood Are Fodder for Sleuths --- Ivana Trump's Private Eye." *The Wall Street Journal*, February 1, 1996. See also the movie "The Insider."

The *Journal* reported that

> "Representatives of B&W offered the fruits of their investigation to *The Wall Street Journal*: a 500-page file bearing the title 'The Misconduct of Jeffrey S. Wigand Available in the Public Record.' Subheadings include 'Wigand's Lies About His Residence,' 'Wigand's Lies Under Oath' and 'Other Lies By Wigand.' A close look at the file, and independent research by this newspaper into its key claims, indicates that many of the serious allegations against Mr. Wigand are backed by scant or contradictory evidence. Some of the charges -- including that he pleaded guilty to shoplifting -- are demonstrably untrue."

Shell/BP/Manfred Schlickenrieder/Hakluyt vs. Greenpeace

In 2001, the *Sunday Times* of London reported that the private investigative firm Hackluyt, which has "close links" to the British spy agency MI6, hired a spy named Manfred Schlickenrieder to infiltrate Greenpeace on behalf of oil companies, including Shell and BP.[106] According to the Sunday Times, Schlickenrieder "posed as a left-wing sympathiser and film maker" to "betray plans of Greenpeace's activities against oil giants…. One of his assignments from Hakluyt was to gather information about the movements of the motor vessel Greenpeace in the north Atlantic."

McDonald's vs. London Greenpeace

In October 1989, McDonald's hired seven private investigators to infiltrate London Greenpeace. According to the *Los Angeles Times*, the infiltrators "took notes, followed organizers to their homes, stole letters and, to demonstrate their bona fides, eagerly volunteered to distribute the fact sheet denouncing the company that had secretly hired them."[107]

---

[106] Maurice Chittenden and Nicholas Rufford, "MI6 'Firm' Spied on Green Groups." *The Sunday Times*, June 17, 2011. See also Chapter 6 of Eveline Lubbers, *Secret Manoeuvres in the Dark: Corporate and Police Spying on Activists.* (London: Pluto Press, 2012).

[107] Alexander Cockburn, "Making Mincemeat Of McDonald's." *Los Angeles Times*, July 18, 1996. Jonathan Calvert, "Cloaks, Daggers and MS X Appeal." *The Observer*, January 26, 1997. See also Chapter 4 of Eveline Lubbers, *Secret Manoeuvres in the Dark: Corporate and Police Spying on Activists.* (London: Pluto Press, 2012).

Stratfor

On February 27, 2012, the non-profit media organization WikiLeaks began releasing emails from the Texas-based private intelligence firm Stratfor,[108] showing that it had conducted espionage against human rights, animal rights and environmental groups, on behalf of companies such as Coca-Cola and Dow Chemical.[109]

Coca-Cola and Stratfor vs. People for the Ethical Treatment of Animals

In June 2009, Stratfor responded to a set of questions from a Coca-Cola executive, Van C. Wilberding, who was "looking at PETA [People for the Ethical Treatment of Animals] and the potential for protests at the [upcoming 2010] Vancouver Olympics..."[110] Coca-Cola was a major sponsor of those Olympic games. Among other things, Coca-Cola asked Stratfor to investigate "To what extent are the actions of PETA in one country controlled by an oversight board/governing body?" and "What is PETA's methodology for planning and executing activism?" Stratfor's vice president of intelligence, Fred Burton, responded that "The FBI has a classified investigation on PETA operatives. I'll see what I can uncover." [111] It is unclear what, if any, information Stratfor provided to Coca-Cola regarding this matter or how it responded to Coca-Cola's other questions.

Dow Chemical and Stratfor vs. Bhopal justice activists

In the evening of December 2, 1984, an explosion at the Union Carbide chemical plant in Bhopal, India released clouds of the toxic gas methyl isocyanate, in what was probably the world's most deadly industrial disaster. No one really knows how many people were killed on that night and subsequently; recent estimates from the Indian government have ranged from 15,000 to 16,000.[112] However, these victims were never adequately compensated. In 2001, Union Carbide became a wholly owned subsidiary of Dow Chemical.

---

[108] Stratfor has received $700,000 in 49 federal contracts since 2008, including 48 contracts with the Department of Defense, according to USASpending.gov (accessed October 28, 2013.)

[109] http://wikileaks.org/the-gifiles.html

[110] Alexi Mostrous, David Sanderson and James Bone, "WikiLeaks Reveals Spycraft Secrets of the 'Shadow CIA.'" *The Times* (of London), February 28, 2012. WikiLeaks http://wikileaks.org/gifiles/docs/5447352_re-peta-.html

[111] WikiLeaks. http://wikileaks.org/gifiles/docs/5282628_re-public-policy-question-for-coca-cola-.html. See also Peter Ludlow, "The Real War on Reality." *New York Times*, June 14, 2013.

[112] Deshdeep Saxena, "Bhopal Gas Tragedy: 27 Years on, Death Toll Still Unknown." *Times of India*, October 29, 2011.

In February 2012, WikiLeaks revealed emails showing that Dow Chemical hired Stratfor to monitor Bhopal justice activists, including the Yes Men.[113]

Stratfor and the Texas Department of Public Safety vs. Occupy Austin and Deep Green Resistance

In November 2011, a Stratfor operative named Korena Zucha recounted that she had a "new source" who was providing her with information about an environmental organization named Deep Green Resistance. She identified the source as a "Texas DPS agent," meaning an agent of the Texas Department of Public Safety.[114]

In an email, the Stratfor operative also reported on her undercover work at Occupy Austin:

> "There is a group you may be familiar with called Deep Green Resistance….Whether anyone in the Fed or elsewhere classifies this group as eco-terror or not, I don't know, but they are nothing but and should be watched….The local Austin chapter was part of the Occupy Austin crowd at city hall, however, things were not "radical" enough for them since they do not believe in working within the system. When I was working U/C on Nov. 5th, some of my contacts told me that at the General Assembly on Nov. 4th, there was some conflict between regular Occupy people and Deep Green."[115]

Monsanto, Blackwater and Total Intelligence Solutions vs. unnamed activists

Jeremy Scahill reported in the *Nation* magazine that the security firm "Blackwater, through Total Intelligence, sought to become the 'intel arm' of Monsanto, offering to provide operatives to infiltrate activist groups organizing against the multinational biotech firm."[116] In recent years, Blackwater has twice been re-named: first as XE Services and again as Academi.[117]

---

[113] WikiLeaks, http://wikileaks.org/gifiles/releasedate/2012-02-27-00-stratford-monitored-bhopal-activists-including.html. See also Ulrik McKnight, "A Wicked Leak: Stratfor, Dow Chemicals, and India." The India Site, 2012. Neha Thirani, "Newswallah: Long Reads Edition." *New York Times* blogs, March 18, 2012. Peter Ludlow, "The Real War on Reality." *New York Times*, June 14, 2013.

[114] http://wikileaks.org/gifiles/docs/184236_re-alpha-insight-us-occupy-austin-and-deep-green-resistance.html

[115] http://wikileaks.org/gifiles/docs/5316058_re-alpha-insight-us-occupy-austin-and-deep-green-resistance.html. See also Michael King, "Strange Bedfellows: Stratfor, the Texas DPS ... and Occupy Austin." *Austin Chronicle*, February 3, 2012.

[116] Jeremy Scahill, "Blackwater's Black Ops." *The Nation*, September 15, 2010.

[117] Academi has received $2.1 billion in federal contracts, including $1.5 billion with the State Department and $607 million with the Defense Department, according to USASpending.gov (accessed October 28, 2013).

According to documents he obtained, Scahill reported in the *Nation* that,

> Through Total Intelligence and the Terrorism Research Center, Blackwater also did business with a range of multinational corporations. According to internal Total Intelligence communications, biotech giant Monsanto—the world's largest supplier of genetically modified seeds—hired the firm in 2008–09. The relationship between the two companies appears to have been solidified in January 2008 when Total Intelligence chair Cofer Black traveled to Zurich to meet with Kevin Wilson, Monsanto's security manager for global issues.
>
> After the meeting in Zurich, Black sent an e-mail to other Blackwater executives, including to [Blackwater owner and founder Erik] Prince and [coordinator of Blackwater's CIA business Enrique 'Ric'] Prado at their Blackwater e-mail addresses. Black wrote that Wilson "understands that we can span collection from internet, to reach out, to boots on the ground on legit basis protecting the Monsanto [brand] name.... Ahead of the curve info and insight/heads up is what he is looking for." Black added that Total Intelligence "would develop into acting as intel arm of Monsanto." Black also noted that Monsanto was concerned about animal rights activists and that they discussed how Blackwater "could have our person(s) actually join [activist] group(s) legally." Black wrote that initial payments to Total Intelligence would be paid out of Monsanto's "generous protection budget" but would eventually become a line item in the company's annual budget. He estimated the potential payments to Total Intelligence at between $100,000 and $500,000. According to documents, Monsanto paid Total Intelligence $127,000 in 2008 and $105,000 in 2009.

Three related stories of espionage

The following three stories, while not strictly about corporate espionage against nonprofit organizations, are closely related to such activity. The first is a case of espionage against an activist who had exposed a powerful politician's role as a former director of a failed savings and loan financial institution. The second is a case of espionage against animal rights activists to uncover the likelihood of protests against corporate exhibitors at one of their conferences. The third concerns extensive and wide-ranging corporate espionage against non-activists.

Henry Hyde, former director of Clyde Federal Savings and Loan vs. Tim Anderson

In 1998, the *Chicago Tribune* reported that Ernie Rizzo, a private investigator, had been hired to investigate Tim Anderson, a former bank consultant and critic of U.S. Rep. Henry Hyde. Hyde was a director of Clyde Federal Savings and Loan between 1981-84.[118] The S&L was declared insolvent in 1990, and cost the taxpayers $67 million, but Hyde was apparently the only director who did not contribute to the settlement. At the time that Rizzo was hired to investigate Anderson, Rep. Hyde was chairman of the U.S. House Judiciary Committee.

Rizzo told the Capitol Hill newspaper *Roll Call* that in 1995 "he was asked by a lawyer working for Hyde to 'find out what this guy Anderson was talking about and what he had.'" Rizzo then posed as a television producer seeking an investigative story about Hyde. Under false pretenses, he accepted 400 pages of documents from Anderson and gave them to one of Hyde's lawyers. According to Rizzo, Anderson "was stirring up things so bad that they [Clyde's directors] could never settle the case, and they wanted to settle it. Anderson kept stirring up reporters."[119] In 1997, the Resolution Trust Corporation finally settled its $17.2 million lawsuit against Clyde's directors for a mere $850,000. Hyde later admitted that his lawyer, James Schirott, had in fact hired Rizzo, and that Hyde had been informed of the results of the investigation.[120]

---

[118] Mike Dorning and Ray Gibson, "Hyde Denies Having Foe Investigated." *Chicago Tribune*, October 18, 1998.
[119] Damon Chappie, "Private Eye's Work Linked To Hyde Investigator Posed As Journalist To Fool Rep.'s Critic." *Roll Call*, October 26, 1998.
[120] Damon Chappie, "Hyde Admits Lawyer Paid for Private Investigator's Work." *Roll Call*, October 29, 1998. Douglas Frantz, "Plenty of Dirty Jobs in Politics and a New Breed of Diggers." *The New York Times*, July 6, 1999.

Society of Toxicology and Information Network Associates vs. animal rights activists

The Society of Toxicology is a "professional and scholarly organization of scientists from academic institutions, government, and industry..."[121] In 2008, the organization planned to hold its annual conference in Seattle, but was concerned about the potential for protests against exhibitors, including Huntingdon Life Sciences. So, it commissioned a "threat analysis" by Information Network Associates, which was founded by a former FBI special agent as an "investigative and security solutions provider."[122] The Society of Toxicology asked Information Network Associates to evaluate the potential for protests and disruptions at the event. INA's 12-page "threat analysis" includes, among many other things, references to the activists' academic and private lives, including who was dating whom.[123]

News Corp./News International/News UK/News of the World

During the last seven years, News Corp., its CEO Rupert Murdoch, and its subsidiary News International[124] have been increasingly engulfed in a sprawling scandal related to illegal hacking of telephone voicemails. Some of the investigations into this matter are ongoing. Following are some of the key events in this developing story.

In 2006, Clive Goodman, the royal editor at *News of the World*, a now-defunct newspaper owned by News Corp., pleaded guilty to intercepting phone messages regarding the British Royal Family. A private investigator hired by *News of the World*, Glenn Mulcaire, also pleaded guilty.[125]

On April 8th, 2011, News International, a subsidiary of News Corp. and parent company of *News of the World*, apologized and offered compensation to eight people whose phone voicemails were hacked, including the actress Sienna Miller and Tessa Jowell, a former U.K. cabinet minister.[126]

---

[121] Society of Toxicology website. http://www.toxicology.org/gp/aboutsot.asp
[122] Information Network Associates website. http://www.ina-inc.com/about-us.php. Information Networks Associates has received $3.1 million in 61 federal contracts, including 21 with the Department of Homeland Security, and 8 with the Department of Defense, according to USASpending.gov (accessed October 28, 2013.)
[123] Will Potter, "Corporations Tracking Who Activists Are Dating." Green is the New Red, June 6, 2008. The Information Network Associates "threat analysis" is available at: http://www.greenisthenewred.com/blog/wp-content/Images/ina_toxexpo_threat.pdf.
[124] On June 26, 2013, News International re-named itself News UK. "News International Changes Name to News UK." *BBC*, June 26, 2013.
[125] Jemima Kiss, "Goodman Pleads Guilty." *Guardian*, November 29, 2006.
[126] James Robinson, "Phone Hacking: NI to Apologise to Victims Including Sienna Miller." *Guardian*, April 8, 2011.

On July 4th, 2011 the *Guardian* reported that *News of The World* hired private investigators to hack the voicemails of Milly Dowler, a missing schoolgirl. Dowler had been murdered, but when *News of the World* deleted some of her voicemails, it gave her family false hope that she might be alive. The voicemail deletions interfered with the police investigation of her death. Her family called the voicemail hacking "heinous" and "despicable."[127]

On July 7th, 2011 the *Daily Telegraph* reported that Glenn Mulcaire, the private investigator working for *News of the World*, may have hacked the voicemails of relatives of soldiers killed in Iraq and Afghanistan.[128]

Also on July 7th, the head detective sifting through the files of Glenn Mulcaire told the *Guardian* that more than 4,000 people may have been targeted with phone hacking.[129]

On July 11th, the *Daily Mirror* reported that *News of the World* had asked a private investigator to "hack into the 9/11 victims' private phone data" and that "journalists asked him to access records showing the calls that had been made to and from the mobile phones belonging to the victims and their relatives." The private investigator, a former New York City police officer, declined the job because "He knew how insensitive such research would be, and how bad it would look."[130]

On July 13, British Prime Minister David Cameron established the Leveson Inquiry to investigate the roles of the media and the police in the phone hacking scandal.[131]

On July 28th, the *Guardian* reported that "Sara Payne, whose eight-year-old daughter Sarah was abducted and murdered in July 2000, has been told by Scotland Yard that they have found evidence to suggest she was targeted by the *News of the World*'s investigator Glenn Mulcaire, who specialised in hacking voicemail."[132]

On August 16th, a British House of Commons committee released a 2007 letter by former *News of the World* royal editor Clive Goodman alleging a cover-up of the phone hacking scandal at *News of the World*. The *Guardian* reports that

---

[127] Nick Davies and Amelia Hill, "Missing Milly Dowler's Voicemail Was Hacked by News of the World." *Guardian*, July 4, 2011.
[128] Mark Hughes, Duncan Gardham, John Bingham and Andy Bloxham, "Phone Hacking: Families of War Dead 'Targeted' by News of the World." *The Daily Telegraph*, July 7, 2011.
[129] Sandra Laville, "Phone Hacking Victims Could Number 4,000, Says Senior Detective." *Guardian*, July 7, 2011.
[130] David Collins, "Phone Hacking: 9/11 Victims 'May Have Had Mobiles Tapped by News of the World Reporters.'" *Daily Mirror*, July 7, 2011.
[131] Leveson Inquiry website at http://www.levesoninquiry.org.uk/.
[132] Nick Davies and Amelia Hill, "News of the World Targeted Phone of Sarah Payne's Mother." *Guardian*, July 28, 2011.

> "Goodman claims that phone hacking was 'widely discussed' at editorial meetings at the paper until [former *News of the World* editor] Coulson himself banned further references to it; that Coulson offered to let him keep his job if he agreed not to implicate the paper in hacking when he came to court; and that his own hacking was carried out with 'the full knowledge and support' of other senior journalists, whom he named."[133]

On July 23, 2012, Leveson Inquiry Deputy Assistant Commissioner Sue Akers testified that, regarding victims of phone hacking, "In total it is believed that there are 4,775 such 'potential' victims, of which 1081 have some additional factor which means we consider them likely to have been victims. These factors include audio recording of voicemail messages, PIN numbers and/or calls to Unique Voicemail Numbers."[134] Akers also testified that the investigation "discovered instances where staff at NI [News International] titles appear to have been in possession of material downloaded or otherwise obtained from stolen mobile telephones."[135]

The FBI was or is conducting a preliminary investigation of whether News Corp. violated any U.S. laws in the phone hacking scandal. News Corp. is headquartered in New York City and incorporated in Delaware. According to the *Associated Press*, the FBI investigation includes whether News Corp. employees or contractors may have bribed police officers, in violation of the Foreign Corrupt Practices Act; whether *News of The World* hacked the phone data of relatives of 9/11 victims; and whether the actor Jude Law had his phone hacked while in the United States.[136] The Department of Justice is also investigating whether News America Marketing, a News Corp. subsidiary, "repeatedly hacked" and stole key financial information from one of its competitors, Floorgraphics, an advertising firm based in New Jersey.[137] News Corp. settled a civil lawsuit on this matter for $29.5 million, and subsequently purchased Floorgraphics.[138]

---

[133] Nick Davies, "Phone Hacking: News of the World Reporter's Letter Reveals Cover-Up." *Guardian*, August 16, 2011. The text of Goodman's letter is at: http://www.guardian.co.uk/media/interactive/2011/aug/16/clive-goodman-letter-phone-hacking.

[134] Third Witness Statement of DAC Sue Akers, Leveson Inquiry. July 23, 2012, at 12. http://www.levesoninquiry.org.uk/wp-content/uploads/2012/07/Third-Witness-Statement-of-DAC-Sue-Akers.pdf. See also Josh Halliday and Dugald Baird, "Leveson Inquiry: Sue Akers - As It Happened." *Guardian*, July 23, 2012.

[135] Third Witness Statement of DAC Sue Akers, Leveson Inquiry. July 23, 2012, at 10.

[136] Pete Yost, "FBI Inquiry of Murdoch's Empire: Reliance on Brits." *Associated Press*, July 25, 2011.

[137] Michael Isikoff, "US Looks Into Alleged Hacking by News Corp.'s Ad Arm." *MSNBC*, July 22, 2011.

[138] For a brief review of News Corp's history of corporate espionage and anticompetitive behavior, see David Carr, "Troubles That Money Can't Dispel." *The New York Times*, July 17, 2011. See also Braden Goyette, "What's the Deal With News Corps Other, U.S.-Based, Hacking Scandal?" *ProPublica*, July 22, 2011.

On August 16, 2013, *Reuters* reported that "London police are actively investigating Rupert Murdoch's British newspaper business for possible criminal violations over allegations of phone-hacking and illegal payments to public officials by its journalists…"[139]

On September 18, 2013, the *Daily Telegraph* reported that U.S. Senator Jay Rockefeller, chairman of the Committee on Commerce, Science and Transportation, "visited News Corp's London headquarters earlier this year, in preparation for a potential Senate investigation." According to the *Daily Telegraph*,

> The Senate committee is unwilling to launch a full-scale investigation into the alleged wrongdoing until after a series of criminal trials of former News Corp staff, due to begin next month. However, Senator Rockefeller is understood to be keen to amass as much evidence as possible ahead of the trials, so that the committee can launch a potential investigation once criminal proceedings have finished…. Last year, he wrote to Lord Justice Leveson requesting any evidence suggesting criminal conduct had occurred in the US, involved US citizens or fallen within the jurisdiction of US laws. The FBI and DoJ are currently investigating any potential violations of the Foreign Corrupt Practices Act (FCPA). However, News Corp could fall foul of other laws if journalists are found to have intercepted voicemails on US soil.[140]

---

[139] Michael Holden and Mark Hosenball, "Murdoch's UK Unit Could Face Corporate Hacking Charges: Source." *Reuters*, August 16, 2013. Roy Greenslade, "Rupert Murdoch's company under investigation on 'corporate charge.'" *Guardian*, August 17, 2013.
[140] Katherine Rushton, "US Senator Visited News Corp's London HQ Ahead of Possible Inquiry." *Daily Telegraph*, September 18, 2013.

FBI investigations of nonprofit organizations

During the last dozen years, the FBI has improperly spied on or investigated nonprofit organizations and activists affiliated with them.[141] The FBI also made false statements about one of these incidents to Congress, the media and the public.

Following a string of news articles about FBI investigations of nonprofit advocacy groups, some Members of Congress requested that the Inspector General of the Department of Justice review these cases. The Office of the Inspector General issued its report in September 2010, regarding FBI investigations between 2001-06. The report was sharply critical of the FBI. The Office of the Inspector General

> "concluded that the factual basis of opening some of the investigations of individuals affiliated with the groups was factually weak….In some cases, we also found that the FBI extended the duration of investigations involving advocacy groups or their members without adequate basis…. In some cases, the FBI classified some of its investigations relating to nonviolent civil disobedience under its "Acts of Terrorism" classification." [142]

In particular, the Office of the Inspector General concluded that:

- The FBI's investigation of the Thomas Merton Center ("Pittsburgh's peace and social justice center") and the FBI's misstatements about it "raised the most troubling issues in this review."[143] The OIG report noted that an FBI agent was directed to attend a Pittsburgh peace rally sponsored by the Merton Center. The agent wrote a short report on it, which bore the synopsis line "[t]o report results of investigation of Pittsburgh anti-war activity."[144] The OIG report stated that it found this FBI report "extremely troubling on its face. It described no legitimate purpose for the FBI to attend the event. It created a strong impression that the FBI's reason for being there was to monitor the First Amendment activities of persons with anti-war views. It supplied no evidence or even suspicion that any criminal or terrorist

---

[141] The FBI has a record of conducting operations designed to surveil, disrupt and discredit activists and nonprofit organizations. See, for example, histories of COINTELPRO from 1956-71, such as James Kirkpatrick Davis, *Spying on America: The FBI's Domestic Counterintelligence Program*. (Westport, CT: Praeger Publishers, 1992).
[142] "A Review of the FBI's Investigations of Certain Domestic Advocacy Groups." Oversight and Review Division, Office of the Inspector General, U.S. Department of Justice, September, 2010, at 190. See also Richard A. Serrano, "FBI Improperly Investigated Activists, Justice Department Review Finds." *Los Angeles Times*, September 21, 2010. Amy Goodman, "FBI Raids and the Criminalization of Dissent." *The Oregonian*, October 1, 2010.
[143] OIG report at 174.
[144] OIG report at 30.

element was associated with the Merton Center or likely to be present at the event."[145]

- "[T]he FBI's statements to Congress and the public about the reason the agent attended the event [Pittsburgh peace rally] were inaccurate and misleading….the FBI stated in a press response and [FBI] Director Mueller stated in Congressional testimony that the FBI's surveillance at the event was based on specific information from an ongoing investigation and conducted to identify a particular individual. These statements were not true. We found no evidence that the FBI had any information at the time of the event that any terrorism subject would be present at the event. Instead, we found that FBI personnel created two inconsistent and erroneous explanations of the surveillance of the anti-war rally, stating inaccurately that the surveillance was a response to information that certain persons of interest in international terrorism matters would be present."[146]

- "[T]he factual predication for the [FBI's] preliminary inquiries…for a federal crime was thin"[147] regarding members of the Pittsburgh Organizing Group, an "affiliate" of the Thomas Merton Center. The POG was planning to protest the November 2003 Free Trade of the Americas meetings in Miami.

- Regarding an FBI agent's recruitment of a source to surveil the POG, "the agent's purpose in recruiting this source…was to establish his participation in the source program, not to prevent or detect terrorism. Because of this improper purpose, we concluded that the FBI's collection of information about POG members' First Amendment activities was not 'pertinent to and within the scope of an authorized law enforcement activity' and therefore raised serious questions under the Privacy Act, the Attorney General's Guidelines, and FBI policy."[148]

- Regarding the FBI's investigation of a staff member of People for the Ethical Treatment of Animals, "The Field Division's decision to operate the case as a full investigation contributed to the case remaining open for 6 years. We concluded that the lengthy duration of the investigation was unreasonable and was inconsistent with FBI policy requiring that an investigation with potential impacts on First Amendment activity 'not be permitted to extend beyond the point at which its underlying justification no longer exists.'"`[149]

[145] OIG report at 59.
[146] OIG report at 176.
[147] OIG report at 179.
[148] OIG report at 179.
[149] OIG report at 181.

- Regarding the FBI's investigation of PETA itself, "The investigation remained open for a total of 15 months, during which time the case received 3 90-day extensions…we questioned the factual basis for the third extension."[150]

- "We identified one PETA-related case that we believe did not have a sufficient factual basis even for a preliminary inquiry."[151]

- Regarding an FBI investigation of Greenpeace and its members, "the FBI articulated little or no basis for suspecting a violation of any federal criminal statute….the FBI's opening EC [electronic communication] did not articulate any basis to suspect that they were planning any federal crimes….We also found that the FBI kept this investigation open for over 3 years, long past the corporate shareholder meetings that the subjects were supposedly planning to disrupt….We concluded that the investigation was kept open 'beyond the point at which its underlying justification no longer existed,' which was inconsistent with the FBI's Manual of Investigative and Operational Guidelines (MIOG)."[152]

- Regarding the investigation of the Catholic Worker and its members, "the FBI's classification of one of these matters under the Acts of Terrorism classification was inappropriate, because the acts in question (trespass on a military facility) did not include the use of violence or force."[153]

[150] OIG report at 181.
[151] OIG report at 182.
[152] OIG report at 182-3.
[153] OIG report at 185.

Surveillance of the Occupy Wall Street movement

There are numerous news accounts and reports of local police, Department of Homeland Security and FBI surveillance of the Occupy Wall Street movement. For example, Matthew Rothschild of the *Progressive* magazine reported that:

> "Over the last few years, the Department of Homeland Security and local law enforcement officers have engaged in widespread domestic spying on Occupy Wall Street activists, among others, on the shaky premise that these activists pose a terrorist threat. Often, Homeland Security and other law enforcement agencies have coordinated with the private sector, working on behalf of, or in cooperation with, Wall Street firms and other companies the protesters have criticized….The documents reveal many instances of such misdirected work by law enforcement around the country. The picture they paint of law enforcement in the Phoenix area is a case in point. The police departments there, working with a statewide fusion center and heavily financed by the Department of Homeland Security, devoted tremendous resources to tracking and infiltrating Occupy Phoenix and other activist groups."[154]

Similarly, in March 2012, the *New York Times* reported that "For the last few months, protest organizers say, police officers or detectives have been posted outside buildings where private meetings were taking place, have visited the homes of organizers and have questioned protesters arrested on minor charges." It tells the story of four people who were arrested, strip-searched and questioned about Occupy protests, even though they were more than a dozen blocks away from an Occupy Wall Street "day of action."[155]

---

[154] Matthew Rothschild, "Spying on Occupy Activists." *The Progressive*, June 2013. See also Michael Hastings, "Exclusive: Homeland Security Kept Tabs on Occupy Wall Street." *Rolling Stone*, February 28, 2012. Jason Cherkis and Zach Carter, "FBI Surveillance of Occupy Wall Street Detailed." *Huffington Post*, January 5, 2013. Dominique Debucquoy-Dodley, "FBI Considered Occupy Movement Potential Threat, Documents Say." *CNN*, December 27, 2012. Spencer Mandel, "I Spy an Occupy: Obama's DHS Surveils Legit Protesters." *WhoWhatWhy*, May 21, 2012. Nick Pinto, "Occupy's Undercover Cop: 'Shady,' Ubiquitous, Willing To Get Arrested." *Gothamist*, October 10, 2013. Lisa Graves, "How the Government Targeted Occupy; The United States Spent Millions Spying on Anti-corporate Activists." *In These Times*, May 21, 2013. Michael Isikoff, "Unaware of Tsarnaev Warnings, Boston Counterterror Unit Tracked Protesters." *NBC News*, May 10, 2013. Todd Gitlin, "The Wonderful American World of Informers and Agents Provocateurs." *Tom's Dispatch*, June 27, 2013. Beau Hodai, "Dissent or Terror: How the Nation's Counter Terrorism Apparatus, In Partnership With Corporate America, Turned on Occupy Wall Street." Center for Media and Democracy and DBA Press, May 20, 2013.

[155] Colin Moynihan, "Wall Street Protesters Complain of Police Surveillance." *New York Times*, March 11, 2012.

InfraGard: an FBI-corporate intelligence partnership

Given the well-documented abuses both by corporations and the FBI in spying on nonprofits, the question arises whether the secretive FBI-corporate intelligence partnership called InfraGard is or could become another vehicle or tool for unethical or illegal espionage against nonprofit organizations.

The cover of the March 2008 issue of *The Progressive* featured an article about InfraGard, a little-known partnership between private industry, the FBI and the Department of Homeland Security.[156] As of then, InfraGard claimed the participation of "more than 23,000 representatives of private industry," including 350 of the Fortune 500 companies. The InfraGard website claims that its "primary focus…is to share actionable intelligence information for investigative purposes."[157]

According to *The Progressive*,

> "One of the advantages of InfraGard, according to its leading members, is that the FBI gives them a heads-up on a secure portal about any threatening information related to infrastructure disruption or terrorism…. 'We get very easy access to secure information that only goes to InfraGard members,' [Chairman of the Board of Directors of the InfraGard National Members Alliance Phyllis] Schneck says. 'People are happy to be in the know.'…. In return for being in the know, InfraGard members cooperate with the FBI and Homeland Security. 'InfraGard members have contributed to about 100 FBI cases,' Schneck says.[158]

The American Civil Liberties Union is concerned about the special advantages granted to corporations under InfraGard. According to the ACLU's Jay Stanley,

> "'The FBI should not be creating a privileged class of Americans who get special treatment….There's no 'business class' in law enforcement. If there's information the FBI can share with 22,000 corporate bigwigs, why don't they just share it with the public? That's who their real 'special relationship' is supposed to be with. Secrecy is not a party favor to be given out to friends….This bears a disturbing resemblance to the FBI's handing out 'goodies' to corporations in return for folding them into its domestic surveillance machinery.'"[159]

---

[156] Matthew Rothschild, "The FBI Deputizes Business." *The Progressive*, March, 2008.
[157] http://www.infragard.net/faq.php?mn=1&sm=1-2.
[158] Matthew Rothschild, "The FBI Deputizes Business." *The Progressive*, March, 2008.
[159] Matthew Rothschild, "The FBI Deputizes Business." *The Progressive*, March, 2008.

Frequently asked questions about corporate espionage

How common is corporate espionage against nonprofits?

We don't really know. Here's what we do know.

Most major companies have created an institutionalized internal chief security position – a chief intelligence officer of some sort. These people often start by asking the question: what "threats" exist to our company? In some cases – but we don't know how many -- corporations identify nonprofit organizations as "threats." They may research the nonprofits by accessing public records and news stories, or consulting public relations firms. But if they find the "threat" serious enough, they may wish to obtain human, physical or electronic intelligence about the organization's plans and activities. And if the corporation is desperate enough, and its ethics are pliable enough, its leaders may even conduct unethical or illegal intelligence-gathering against nonprofits.

Most of the cases of corporate espionage we know about in recent years have been uncovered by accident. There has been no comprehensive, systematic effort by federal or state government to determine how much corporate espionage is actually occurring, and what tactics are being used. It is likely that corporate espionage against nonprofits occurs much more often than is known.

Regarding corporate espionage in the United Kingdom, the *Guardian* reported that "Privately, senior officers claim there are 'without question' more corporate spies embedded in the protest movement than police officers. Among their number are former police officers cashing in on their surveillance skills for a host of companies that target protesters."[160]

Another estimate of the prevalence of corporate espionage – but perhaps a self-serving one -- comes from Russell Corn, managing director of Diligence, a corporate intelligence agency. Corn says that "private spies make up 25 per cent of every activist camp. 'If you stuck an intercept up near one of those camps, you wouldn't believe the amount of outgoing calls after every meeting saying, 'Tomorrow we're going to cut the fence',' he smiles. 'Easily one in four of the people there are taking the corporate shilling.'"[161]

Who actually conducts the espionage?

When a nonprofit campaign is so successful that it may impair a company's profits or reputation, companies may employ their own in-house espionage capabilities, or they may retain the services of an intermediary with experience in espionage. Typically, such

---

[160] Paul Lewis and Rob Evans, "Special Report: Green Groups Targeted Polluters As Corporate Agents Hid In Their Ranks." *Guardian*, February 15, 2011.
[161] Stephen Armstrong, "The New Spies." *New Statesman*, August 7, 2008.

intermediaries are public relations firms, crisis management firms, and law firms. The advantage of an intermediary, from the corporate perspective, is that it provides the appearance of distance between the corporation and its intelligence gathering – in other words, plausible deniability if something goes wrong.

The intermediary may hire a private investigations firm that either has multiple espionage capacities or that specializes in the particular kind of intelligence needed – such as human intelligence and the infiltration of nonprofits, or electronic or physical surveillance. These private investigations firms may subcontract out espionage to experienced operatives, which gives corporations access to specialized talent while further increasing the level of plausible deniability.[162]

What is the extent of involvement of current and former police, CIA, NSA, FBI, Secret Service, and other military, intelligence and law enforcement officials?

One of the troubling aspects of recent corporate espionage against nonprofits is the use of current and former police, current government contractors, and former CIA, NSA, FBI, military, Secret Service and other law enforcement officers.

Even active-duty CIA operatives are allowed to sell their expertise to the highest bidder, "a policy that gives financial firms and hedge funds access to the nation's top-level intelligence talent," writes Eamon Javers. Little is known about the CIA's moonlighting policy, or which corporations have hired current CIA operatives. According to Javers, "There is much about the policy that is unclear, including how many officers have availed themselves of it, how long it has been in place and what types of outside employment have been allowed."[163] Regarding the CIA process for approving moonlighting, U.S. Rep. Anna Eshoo said "My sense is that it is a rubber stamp deal….No one's really looking at it or keeping a close eye on it."[164]

In effect, corporations are now able to replicate in miniature the services of a private CIA, employing active-duty and retired officers from intelligence and/or law enforcement.

Hiring former intelligence, military and law enforcement officials has its advantages. First, these officials may be able to use their status as a shield. For example, current law enforcement officials may be disinclined to investigate or prosecute former intelligence or law enforcement agents. They may be more likely to get a "pass" because of their

---

[162] See, for example, Russell Mokhiber and Robert Weissman, "Corporate Spooks." March 6, 2001.

[163] Eamon Javers, "CIA Moonlights in the Corporate World." *Politico*, February 1, 2010. See also U.S. House of Representatives, Permanent Select Committee on Intelligence. "Annual Threats Assessment, Part I." Hearing transcript, February 3, 2010. Kasie Hunt, "CIA Moonlighting to be Investigated." *Politico*, February 3, 2010. Eamon Javers, *Broker, Trader, Lawyer, Spy*. (New York: HarperCollins, 2010), p. 198.

[164] Eamon Javers, "Rep. Targets CIA Moonlighting." *Politico*, February 23, 2010.

government service. In effect, corporations are hiring that "pass" and sometimes using it to conduct unethical or even illegal intelligence gathering against nonprofits.

Lawlessness committed by this private intelligence and law enforcement capacity, which appears to enjoy near impunity, is a threat to democracy and the rule of law. In essence, corporations are now able to hire a private law enforcement capacity – which is barely constrained by legal and ethical norms -- and use it to subvert or destroy civic groups. This greatly erodes the capacity of the civic sector to countervail the tremendous power of corporate and wealthy elites.[165]

In effect, the revolving door for intelligence, military and law enforcement officials is yet another aspect of the corporate capture of the federal agencies, and another government subsidy for corporations. Taxpayer funds are expended to train the officials who work for the CIA, NSA, Secret Service, military and other intelligence and law enforcement agencies. When these employees leave for employment in the private sector, corporations reap the benefits of this taxpayer-funded education, training and experience. It's a great deal for the companies that hire these former agents, but not for taxpayers.

What techniques are used in corporate espionage against nonprofits?

We may not really know all of them. There may be intelligence-gathering techniques that are used against nonprofits about which there is little or no public knowledge.

We do know that for almost two decades, corporations have employed a wide variety of human, physical and electronic surveillance techniques.

To obtain human intelligence, in the cases that are publicly-known, many corporations have hired spies -- either directly or through intermediaries – who use a false or misleading identity to infiltrate an organization. Often the spy poses as a volunteer or supporter, to secretly harvest information over a long period of time, or as a journalist, to gather a lot of information quickly. The spy may wear a recording device to capture all verbal communication that occurs near him.

---

[165] See James Ridgeway, "The Dirty History of Corporate Spying." *Guardian*, February 15, 2011. "The private detective firms working for corporations can develop information against their own targets and find eager recipients among federal and local law enforcement agencies, some of whose employees end up retiring into private-sector detective work. The corporate spy business thus amounts to a shadow para-law enforcement system that basically can get around any of the safeguards set out in the American legal system; it ought to be subject first to transparency, and then to banning. That's not likely to happen any time soon, but what could happen, and what has been so far unsuccessfully requested of Congress, is a thoroughgoing investigation of this para-legal apparatus with a view to exposing its dangers and figuring out the best way of eliminating its abuses."

To obtain physical intelligence such as documents, the most common technique appears to be dumpster diving: collecting trash and recycling, even from receptacles on the target's property. Such receptacles can be accessed by trespass, or by employing a moonlighting active-duty law enforcement officer, such as a local police officer or state trooper. Corporations may also hire the services of experienced nonprofit infiltrators who may pose as volunteers, to scout out workplaces and to steal documents left unattended or unguarded. Corporate spies may also plant bugs to obtain and transmit verbal communication. Both offices and homes may be targeted for the gathering of physical intelligence.

The techniques of electronic espionage are far too diverse and complex to treat fully in this brief report. However, here is a sketch of the more salient ones.

- **Vulnerability research**. A corporate spy may begin an electronic intelligence gathering effort by assessing the comparative vulnerabilities of a nonprofit's computers, networks and electronic communications.

- **Computer hacking**. There are many different techniques available to corporate spies who wish to hack a computer or computer network. Some of the more obvious ones may include vulnerability scanning (checking computers and networks for known security flaws), persistent software implants and creation of custom malware, password cracking, phishing (obtaining passwords by posing as a trustworthy entity), Trojan horses (establishing a back door into a computer or network that can be exploited later) and key loggers (recording of all keystrokes on a computer for later retrieval).

- **Obtaining phone records**. This often involves the practice of pretexting, or using a false identity or pretenses to trick a phone provider into releasing records of phone calls. Corporate spies may also breach online account administration tools that are made available to phone customers.

- **Wiretapping**. Corporate spies may tap phones in many ways, including implanting bugs in a handset or anywhere along a phone line, tapping outside phone boxes and using radio scanners.

- **Phone voicemail hacking**. Some phone voicemail systems can be easily hacked via web-based spoofing services, which corporate spies can use to make their calls seem like they are coming from the voicemail that they are hacking into.

- **Theft of computers**. Computer data can be obtained by theft – especially of laptops.

What other offensive tactics can corporate spies use?

- **Disinformation**. Corporate spies may create and disseminate disinformation to create dissention within an organization, or to discredit an organization. They may also create false information that, if released by the organization to the public, would damage the organization's credibility.

- **Investigating the private lives of activists** -- including their spouses, children, religious activities -- to gain leverage over them.

- **Blackmail**. Corporations can blackmail activists to try to force them to stop their campaign against a corporation.

- **Creation of false dossiers**. Corporations can hire law firms or private investigators to compile false or misleading dossiers to discredit an activist or whistleblower.

Which nonprofits get targeted for corporate espionage?

In general, there are two preconditions for a nonprofit to be targeted with corporate espionage.

First, it requires a corporation that is willing to use the tools of espionage and the risks associated with it.

Second, it requires a nonprofit that impairs or at least threatens a company's assets or image sufficiently. Mark Floegel of Greenpeace says that Greenpeace has been repeatedly targeted for espionage because "We're effective at what we do." But he also notes that some PR firms (which sometimes subcontract with private detective firms) "have a symbiotic relationship with Greenpeace." He says that on several occasions, PR firms have contacted the corporate targets of Greenpeace by saying "Don't let Greenpeace embarrass you." Floegel says that Greenpeace is "really good for the PR economy."

How much do companies spend on espionage against nonprofits?

We don't really know.

There are indications that some companies and trade associations pay millions for espionage against nonprofit organizations. For example, Berico Technologies, HB Gary Federal and Palantir Technologies proposed a $2 million monthly budget to Hunton & Williams for a U.S. Chamber of Commerce campaign against U.S. Chamber Watch and other critics of the Chamber of Commerce.[166]

[166] http://images2.americanprogress.org/ThinkProgress/themisplan.pdf.

Policy recommendations: How to protect nonprofit organizations from corporate espionage

The failure to hold corporations or their contractors accountable for corporate espionage against nonprofits may well encourage other corporations to conduct espionage against nonprofits.

Self-regulation of corporate espionage – by corporations themselves, their private investigators, public relations firms, law firms, and their contractors – is an abject failure. Based on the cases and activities reviewed in this report, it is clear that these firms are either unwilling or unable to police themselves adequately to prevent illegal or unethical espionage against nonprofit organizations.

There are many things that can be done to protect both nonprofits and our democracy from illegal or unethical corporate espionage.

1. Congress should hold hearings on corporate espionage against nonprofits. Congressional committees should subpoena documents and testimony from corporations, PR firms, private detective firms, law firms and contractors known or suspected of conducting espionage against nonprofits. They should ask questions of these firms, such as:

    - Which nonprofits have you (or your contractors or subcontractors) conducted espionage against?

    - What espionage tactics have you (or your contractors or subcontractors) used against nonprofits?

    - Have you (or your contractors or subcontractors) ever taken any actions that may have been unethical, illegal or potentially illegal? If so, what were they?

    - How much have you paid to conduct espionage against nonprofits? How much were you paid to conduct espionage against nonprofits?

    - Have you ever employed the services of current or former police, CIA, NSA, FBI, Secret Service military, and/or other law enforcement or intelligence agents? What kinds of espionage tactics have they used?

    - Has any current or former law or intelligence official ever used their official position or official status on your behalf? If so, how?

2. Congress should also hold hearings on moonlighting by federal intelligence and law enforcement officials to assist in corporate intelligence gathering activities. Members of Congress should ask these questions:

- How often do active-duty or retired intelligence or law enforcement officials participate in corporate espionage against nonprofits?

- What is the nature of the review conducted by Designated Agency Ethics Officials (DAEOs) and/or other agency officials regarding moonlighting to conduct corporate espionage against nonprofits?

- How often, if ever, do DAEOs or other agency officials disallow intelligence or law enforcement staff from engaging in specific moonlighting projects?

- Are there any restrictions on contracting with private intelligence companies that conduct espionage against American citizens on behalf of corporations?

- What prevents government agencies from hiring individuals with a record of violating citizens' right to privacy or other activities that violate Americans' constitutional rights?

3. Law enforcement – especially the U.S. Department of Justice – should prioritize investigating corporate espionage against nonprofit organizations. This could easily have a potent deterrent effect, as well as bringing wrongdoers to justice.

4. Congress should enact a "Citizen-Group Espionage Act" to criminalize the theft of confidential, noneconomic information.[167] Such a statute, if enforced, would also be a powerful deterrent to corporate espionage against nonprofits.

5. Congress and state legislatures should prohibit commercial dumpster diving -- the practice of rummaging through trash to gain access to trade secrets and other valuable or confidential information.

6. Congress and state legislatures should prohibit active duty law enforcement officials – including state and local police, FBI, NSA, CIA, US military and Secret Service -- from conducting corporate espionage against nonprofit organizations.

7. Congress should legislate full transparency regarding espionage against nonprofits, by requiring all publicly-traded corporations that expend funds – either directly or indirectly via law firms, PR firms or private investigators – to conduct espionage against nonprofits to disclose the cost, tactics and targets of the espionage.

8. Congress and state legislatures should require all contractors with law enforcement or intelligence agencies -- including state and local police, FBI, NSA, CIA, US military and Secret Service – to affirm in their contracts that they will not conduct espionage

[167] Andrew Frohlich, "Volunteering to Deceive: Criminalizing Citizen-Group Espionage." *George Washington Law Review*, April, 2010. 78 Geo. Wash. L. Rev. 668.

against nonprofit organizations.

9. Congress should direct the Inspector General of the Department of Justice to prepare an annual report on law enforcement surveillance of nonprofits. Special attention should be given to the evidence used to open investigations and to how long investigations remain open, to ensure that government resources are being used for actual law and order and not as taxpayer-funded corporate security.

10. Congress and state legislatures should enact legislation sanctioning any police officer who abuses his or her authority when moonlighting (i.e., "using the badge" to gain access to areas or information unavailable to the public).

11. Leaders of U.S. law enforcement and intelligence agencies should warn both active duty and retired members of their agencies that corporate espionage against nonprofit organizations is unethical, intolerable and often illegal.

12. Foundations and private donors should establish and fund free-of-charge nonprofit security advisors, who can dispense advice to nonprofits about how to protect against corporate espionage.

For further reading

Jessica Bell and Dan Spalding, "Security Culture for Activists." The Ruckus Society. A basic primer on how activists can protect themselves from government and corporate espionage.

Eamon Javers, *Broker, Trader, Lawyer, Spy*. (New York: HarperCollins, 2010).

Brian Glick, *War at Home: Covert Action Against U.S. Activists and What We Can Do About It*. (Cambridge, MA: South End Press, 1989).

Tom Devine and Tarek F. Maassarani, *The Corporate Whistleblower's Survival Guide*. (San Francisco, Berrett-Koehler Publishers, 2011).

John Stauber and Sheldon Rampton, *Toxic Sludge is Good For You: Lies, Damn Lies and the Public Relations Industry*. (Monroe, ME: Common Courage Press, 1995.) See especially chapter 5, "Spies for Hire."

Eveline Lubbers, *Secret Manoeuvres in the Dark: Corporate and Police Spying on Activists.* (London: Pluto Press, 2012).

Heidi Boghosian, *Spying on Democracy: Government Surveillance, Corporate Power and Public Resistance*. (San Francisco: City Lights Books, 2013).

Organizations

The Electronic Frontier Foundation has an assortment of useful materials regarding electronic communications security. www.eff.org. See especially materials on "Surveillance Self-Defense." https://ssd.eff.org/.

Over the years, the Center for Media and Democracy has written many articles about corporate spying on nonprofit organizations. www.prwatch.org. See also their resources on SourceWatch. www.sourcewatch.org.

Much of what we know about corporate espionage during the last seventeen years was covered – or covered first – in the *Guardian*. www.guardian.co.uk.