

LEVICK

■ EDITION 7

Monthly

JANUARY, 2014

**The Tech
Industry's
NSA
Campaign:**

**Trickier
Than It
Seems**



Contents

- 04** **COVER STORY**
The Tech Industry's NSA Campaign: Trickier Than It Seems
- 08** **CRISIS & REPUTATION**
Buckyballs: Stones Enough to Fight Back
- 12** **DIGITAL ENGAGEMENT**
Hack Attack? -- Preparing for a Social Media Crisis
- 14** **PUBLIC AFFAIRS**
In Youngstown, Fracking Figures Out That Tactics Are Neutral
- 16** **FINANCIALS**
Robocop on the Beat: What the SEC's New Financial Reporting and AQM Initiative May Mean for Public Companies
- 20** **LITIGATION**
The GC's Role in the Digital Revolution: Corporate Campaigns



**The Tech
Industry's NSA
Campaign:**

**Trickier
Than It
Seems**

Richard Levick

Originally Published on forbes.com

Whatever happens, Edward Snowden's dream has come true. As has been observed, the National Security Agency's nemesis hoped at least to set off a debate in which the NSA's massive electronic spying would be challenged. That debate has, of course, been ongoing and predominantly unfavorable to the agency.

Now, in response to documents leaked by Snowden detailing how the NSA garnered data from tech companies under secret court orders, eight technology sector giants have written a new chapter in the debate as they've collaborated aggressively to dispel perceptions that they voluntarily provided government access to significant amounts of user information.

Far from a purely defensive campaign, the companies have launched a shrewd offense, indignantly clamoring for government policy change, and trumpeting their enhanced use of encryption technology to protect user data. Yahoo, for one, says it will encrypt all traffic between its data centers by Q1 of 2014. Google was an early leader here as its similar encryption initiatives were first approved in 2012.

The campaign has won widespread approbation from a variety of sources in and out of the data security industry. Apparently, Americans are shocked, just shocked to learn that their government wants to gather as much information about private citizens as American Internet companies have accumulated. Yes, there is gambling in Casablanca.

The Silicon Valley Eight – AOL, Apple, Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo – effectively packaged their message in an open letter to the President and Congress sent on December 9. As should be expected, these companies have effectively used the digital arena as well as print media to maximize dissemination, including a dedicated website. It's altogether appropriate and reassuring that they be seen doing good instead of just doing it.

They've been additionally shrewd, reinforcing their initiative with resolute public commentary by the likes of Microsoft general counsel Brad Smith, who said in a blog post that the NSA surveillance "threaten[s] to seriously undermine confidence in the security and privacy of online communications." Facebook CEO Mark Zuckerberg sounded a sarcastic note when he responded to NSA assurances that it only gathers data on people outside the U.S. "Wonderful," Zuckerberg said. "That's really helpful to companies that are trying to serve people around the world and really inspire confidence in American Internet companies." Such derisiveness will only enhance consumer confidence in its source.

It's all about passionate advocacy plus practical solutions – the very stuff of corporate heroism. The fact that these companies have crucial economic interests at stake by no means obviates their credibility. To the contrary, such enlightened self-interest only fuels the perception that these companies mean business, that We The People are indeed

their inviolable stakeholders, and that they have no choice but to fight hard on our behalf.

Yet for all that, their communications strategy is not risk-free and the strategic undertow here may well be a mite treacherous. The dark subtext is that, before the NSA fracas began, some of these companies were themselves seen as main threats to the public's data privacy, not because they were helping law enforcement fight terrorism but, rather, helping advertisers hawk goods and services. Attracting advertisers is their core business, after all. Public fear of the private sector forces is not necessarily less obsessing than fear of Big Brother. (Last May, pre-Snowden, I wrote an article in these pages called "Big Google Is Watching You." I must say, it did strike a nerve.)

All of which is not to say that these companies should regret or rethink a strategy that will likely benefit them after all the dust settles, and serve the commonweal as well. It is to say, however that, in their deliberations, they would do well to anticipate a counter-attack, if not from the government than from the very public they're now so impassioned to protect. All those Internet users have longer memories than you might think.

These users, inspired by the December 9 letter, may well redirect their attention and demand that the private companies clean their own houses as well. That, to be sure, will be a major business problem for which the eight companies need to be prepared well in advance, especially since their very business model is based on the

same kind of aggressive accumulation of information for which the NSA has been castigated.

At the heart of their economic anxiety are the global markets and the potential migration of business to foreign-based providers as well as the onerous regulation of U.S. tech companies by foreign governments. The irony is painful as we're supposed to be the democratic soil nourishing Internet communications. Now it's the Chinese who are wary of our Orwellian misuse of technology, or so says Cisco, which projects a 10% quarterly loss based on backlash in China and other "emerging markets."

Yet Cisco, along with numerous other giants, including Oracle and AT&T, did not sign the letter to the government. Their conspicuous and widely reported absence may only encourage perceptions that:

One, while there are eight companies eager to effect reform, the U.S. technology industry as a whole is not signed on.

Two, companies that don't deal directly with consumers are really indifferent to the message, although, inexplicably, Amazon and eBay did not sign either – and declined to say why not.

Three, you never know where big government contracts are likely to compromise private sector commitment to data protection.


So, all things considered, let's not take our chances stateside. In terms of total lost revenue, the cost to U.S. companies is

projected in the billions, and that's only for hosting Internet services and selling remote data storage. It doesn't even include potential lost ad revenue.

So again, what seems an impervious communications strategy has weak links. Not only may the signatories have to answer sooner or later for their own past and present actions, but the current campaign could exacerbate jaundiced perceptions of the U.S. technology sector as a whole.

"The tech giants who issued the statement have broken new ground," Greg Nojeim, senior counsel at the Center for Democracy & Technology, told the press.

That may still be true. "New ground," however, is often littered with landmines. Eight corporate behemoths may have taken a decisive step in the public communications arena, but any such strategy confronts decisive contradiction when it's fundamentally at odds with the business model on which the communicators actually operate.

That's the way the "cookies" sometimes crumble. 



Buckyballs

Stones Enough To Fight Back

Richard Levick

Originally Published on LEVICK Daily

There's a familiar old catchphrase denoting an unwinnable struggle against intractable foes: "Go Fight City Hall!"

Well, on November 13, Craig Zucker announced that he was doing just that by suing the Consumer Product Safety Commission (CPSC), which since February has been trying to hold him personally liable for the full \$57 million cost of recalling Buckyballs. Those are the magnetic desk toys that Zucker invented, and which the CPSC ordered off the market because they pose a safety risk to young children if they swallow them.

Zucker wants an injunction against the agency's demand that, as a principal of the now-defunct company that manufactured the product, he bear the full cost of a product recall. That \$10 million company, Maxfield & Oberton, dissolved in 2012 in the wake of the government's recall order. Zucker's current lawsuit claims the CPSC lacks jurisdiction to target him.

Make no mistake, however – the issues here are far more portentous than any mere squabble over jurisdiction. In fact, Zucker's filing was quickly endorsed by none other than Nancy Nord, the CPSC's former commissioner (2005 to 2013) and acting chairman (2006-09). In an op-ed, Nord decried the recall itself as well as the novel legal move to hold Zucker personally liable. "I hope he wins his suit," she wrote. Such unequivocal support from the Commission's most prominent alumna may suggest that Zucker actually stands a decent chance to win his fight against City Hall.

It is indeed a baleful tale of government overreaching that has enraged both the left and the right, drawing well-deserved fire from such unlikely bedfellows as the Huffington Post and the NGO Cause of Action, which filed the suit on Zucker's behalf.

The overreaching occurred on two fronts. The government's extraordinary action in seeking Zucker's personal liability has rattled the marketplace, but the CPSC's inexplicable behavior during the recall itself raises no less persisting concerns. In situations involving regulatory oversight, the common wisdom espoused by lawyers, and communications consultants, recommends full cooperation with the government to achieve socially responsible aims.

In 2010, I wrote about the CPSC in these pages

as a new regulatory force to reckon with, especially after the commission's powers had been expanded in 2008 and its budget increased to cover the new mandates from Congress. "Whenever businesses deal with regulators, relationships based on trust can produce measurable results in terms of potential fines, lawsuits, etc.," I wrote.

Presumably that counsel is still axiomatic. Yet in this case Craig Zucker was a very model of cooperativeness from the get-go. His company's lawyer was the former head of compliance at the CPSC. In 2011, commission chair Inez Tenenbaum even praised Zucker's company for going beyond compliance to ensure product safety – something businesses are also typically well advised to do. Yet here again all the sagacious best practices and articulated rules about how to deal with regulators finally proved irrelevant.

The CPSC seems to have simply turned on Zucker, targeting Buckyballs after years of mutual collaboration on testing and labeling. The commission has apparently disserved business and itself by betraying the critical trust element that must guide the regulatory dynamic. As a result, one company is out of business and an honest businessman confronts a \$57 million liability.

Meanwhile, the commission held a public meeting as recently as this October in which evidence was presented to mainly confirm that ingesting magnet sets is indeed physically injurious. The recall is hard to justify under any circumstances. As reported, there were only 22 reports of anyone swallowing Buckyballs during a three-year period – one incident per 100,000 sets. The product, labeled "Keep Away from All Children," is therefore statisti-

cally less dangerous than skateboards and tennis balls. The commission did point out that Buckyballs have “low utility to consumers” and “are not necessary to consumers.” Hmm...I hope Big Brother doesn’t come after my hula hoop.

Bad as the recall fact patterns are, it was the personal targeting of Zucker that blew this story well beyond the product manufacturing sector. Possibly, such draconian action was in part catalyzed by an ad campaign Maxfield & Oberton launched after the recall to recruit Beltway supporters, including some derisive finger-pointing at Tenenbaum. Injudicious, perhaps, but we’d hate to believe the CPSC’s regulatory zeal is not tempered by some respect for the First Amendment.

For entrepreneurs and business leaders in all industries, the most chilling element is that, if this case sets any precedent whatsoever, they too could be personally exposed in civil lawsuits for actions the government never even sought to classify as criminal.

According to the “responsible corporate officer” doctrine, which the CPSC is relying on, officers can be criminally liable even if they are unaware of illegal acts. Yet Buckyballs are not even demonstrably dangerous, much less criminal. In fact, it’s still legal to sell the product. Moreover, there’s been virtually no use of “responsible corporate officer” in administrative proceedings that do not include allegations of law-breaking. In one 1975 Supreme Court case, *United States v. Park*, the CEO of a


food retailer was held criminally liable under this doctrine for rodent infestation at the company’s warehouses. But eighteen years later SCOTUS ruled in *Meyer v. Holley* that only ordinary exposure applies absent clear congressional intent in the related statute to hold individual officers liable.

So the fact remains that a regulatory agency, the CPSC, is now trying to make new law and very bad law at that. It gets worse. As Nord points out, the commissioners never even voted to use the responsible corporate officer doctrine against Zucker. The decision

was made by....agency lawyers.

Happily, there is a third, rather more encouraging dimension to this saga: the potential rallying power of the social media. Here we particularly see how that power is sustained by forcing events, which keep the story in high gear. Although Buckyballs continued to sell on the Internet – after retailers were intimidated by the government into dropping the product – Zucker himself expected those online sales to dry up.

Yet the digital momentum was then revived by the CPSC’s outrageous pursuit of Zucker. Now Zucker’s lawsuit should infuse new energy. Meanwhile, Zucker’s website has been an effective tool, raising money for legal bills by selling new magnetic “Liberty Balls” (too big to swallow) and further driving the grassroots message in the process. In just a three-week period, more than 2,200 people bought \$10-to-\$40 sets.



Make no mistake, however – the issues here are far more portentous than any mere squabble over jurisdiction.

Some regulators might respond by redoubling efforts to crush such impertinence. Others might respond by dutifully reexamining their own actions. Let's keep a close eye on which route the CPSC chooses.

It's no doubt cold comfort to Craig Zucker, but in the long run it may be fortunate that the facts in his case are so horrendous. Less conspicuous regulatory overreaching would likely go unpunished, even unnoticed by anyone other than the victims. Here, because the injustice so loudly begs for rebuke, a philosophically diverse public has risen to the defense.

Sometimes, hard cases un-make bad law. **L**

HACK ATTACK?

PREPARING FOR A SOCIAL MEDIA CRISIS

Peter LaMotte

Originally Published on LevickDaily

On April 23, a story went out to two million followers on the AP official Twitter account that there were two explosions at the White House and President Obama was injured. The stock market plunged by almost 150 points in a matter of seconds. The result of a hacking by the Syrian Electronic Army, the false statement was quickly corrected, the compromised Twitter account was shut down and the stock market soon recovered.

Malicious mischief or an issue that should be a major concern throughout any organization? In the case of the AP, the hackers are clearly raising the level of threat by going after the very nature of the brand itself – the credibility of the institution as a trustworthy news source.

As social media becomes a significant part of the organization's brand, the risk of a crisis looms. Some warn that it is no longer a question of if it will happen, but when. In December, it was reported that a cyber-attack emanating from the Nether-

lands broke into at least 2 million accounts and stole passwords at social media outlets including Facebook, Twitter, LinkedIn and Google. More than 93,000 websites were compromised, along with 8,000 Fortune 500 Automatic Data Processing Accounts. Passwords were changed but the damage has not yet been assessed.

How do you prepare against a threat from an enemy that is faceless...that could reside anywhere in the world...whose motives are unknown and whose tactics change faster than the technology used to combat it?

The first defense is to upgrade your overall approach to social media security and your operating procedures. Make sure you have a robust security platform with a two-step authentication process for all social media outlets. The list of those who have access to your accounts should be limited to a few specific people. In the rush for immediacy, don't circumvent the approval process. All images and statements should be pre-approved or at least adhere to guidelines before they go out.

Monitor what's being said about you and be ready to react. Twitter has become a powerful tool not just for marketing and customer service, but also for financial communications.. Bloomberg LP has Twitter feeds that are closely monitored by traders. One false tweet can damage your stock market valuation as well as your reputation.

Schedule posts for a specific day of the week and time. If something appears at an unscheduled time, it is worth investigating the source.

Have a social media crisis communications plan in place and be ready to spring into action. Prepare statements, get immediate turnaround approvals, and use both social and traditional media. Be sure to include some of the newer, emerging social media sites as well as the 'old' favorites like Twitter, Facebook and YouTube.

Scan the external environment. Some social media crises result from our own doing rather than from a malevolent hacker. When the New Town school shooting occurred, Mutual of Omaha had posted a pre-planned tweet about life insurance and the NRA posted a holiday giveaway tweet about – yes guns. The instant a tragic event occurs, all posts deemed inappropriate or offensive should be pulled.

Finally, make social media an integral part of your risk management plan. With a carefully planned strategy, the risk can be mitigated and the potential reward for

your brand can be magnified through new and emerging social media. **L**



In Youngstown, Fracking Figures Out That Tactics Are Neutral

Richard Levick

Originally Published on Forbes.com

After my last post on fracking, it may surprise some readers to learn that I began my career in public affairs advocacy as an environmental activist. I marched against nukes, fought “Big Oil,” and lectured about sustainability three decades before it was “cool.” As long as the villain in the story

was a monolithic energy company, it was always easy to protest and build the “us vs. them” narrative that every strong movement needs.

Thirty years later, that dynamic remains a lynchpin of environmentalism. And it helps explain why voters in Youngstown Ohio bucked a national trend by rejecting

a moratorium on hydraulic fracturing last month. Activism is easy when your opponents are faceless, monolithic corporations. But when you have to go up against real people in the communities you're purportedly trying to save, the job gets a heck of a lot harder.

In Youngstown, it seems we learned that tactics really are neutral after all.

According to numerous media reports, the United Association of Plumbers and Pipefitters Local 396 spent \$74,000 to defeat the Youngstown moratorium, which it saw as a "job killer." That's not a lot of money, even in terms of a targeted, local campaign. It's even less when you consider the ways in which activists utilize relatively inexpensive social media engagement to level the messaging playing field. But the union's impact on the referendum can't be measured in terms of dollars and cents.

This was a rare case in which fracking proponents had a local ally that could echo their messages with emotion, influence, and credibility – at the kitchen table, the supermarket, over the backyard fence, or via industry Facebook and Twitter accounts. That turned the traditional activist narrative on its head. In Youngstown, it was the energy industry that had local interests at heart. Activists were the outsiders seeking to impose their will on a local community. **L**

Robocop on the Beat: What the SEC's New Financial Reporting and AQM Initiative May Mean for Public Companies

Paul Ferrillo

Originally Published on LevickDaily

The following guest post from Christopher L. Garcia, Paul Ferrillo of the Weil, Gotshal & Manges law firm and Matthew Jacques of AlixPartners takes a look at a new information gathering initiative from the SEC. It originally ran on The D&O Diary.

Since her confirmation as Chair of the U.S. Securities and Exchange Commission (“the SEC”), Mary Jo White has made clear that her administration will focus on identifying and investigating accounting abuses at publicly traded companies, a focus that has been echoed by Chairperson White’s co-Directors of Enforcement, George Canellos and Andrew Ceresney. This renewed focus is perhaps unsurprising: whistleblower complaints relating to corporate disclosures far outstrip complaints in other popular enforcement areas, such as insider trading and FCPA, and yet the last several years have witnessed a steady decline in accounting fraud investigations and enforcement action.

Accordingly, on July 2, 2013, the SEC announced two initiatives in the Division of Enforcement designed to support this renewed focus on uncovering and pursuing accounting abuses in public companies:

The Financial Reporting and Audit Task

Force (“the Task Force”), “an expert group of attorneys and accountants” dedicated to detecting fraudulent or improper financial reporting; and

The Center for Risk and Quantitative Analytics, which is dedicated to “employing quantitative data and analysis to high-risk behaviors and transactions” in an effort to detect misconduct.

While the Task Force portends a new era in accounting fraud enforcement by creating a veritable “SWAT Team” tasked with reviewing financial restatements and class action filings, monitoring high risk companies, and conducting street sweeps, the announcement that the SEC is employing “data analytics” to in order to detect indicia of accounting fraud is potentially the more significant development.

First dubbed the “Accounting Quality Model” (“AQM”) by the SEC’s Chief Economist Craig M. Lewis, and later coined “Robocop” by the media, the use of data analytics represents advances in enforcement techniques made possible by a prior SEC compliance initiative called XBRL (eX-

tensible Business Report Language), which mandated a standardized format for public companies to report their results. This article attempts to bring together all of the concepts related to the AQM in an understandable way for directors and officers of public companies. In short, the AQM may mean that companies may receive more frequent inquiries from the SEC based upon the substantive quality of their financial statements alone. Though just one tool in the SEC's enforcement tool box, the SEC's AQM initiative certainly represents how 21st Century information gathering may give the SEC a leg up in detecting accounting fraud.

WHAT IS XBRL?

First, a brief word about XBRL, which has made the SEC's AQM initiative possible. In mid-2009, the SEC mandated the use of XBRL (XBRL was voluntary beginning in 2006) for most companies reporting financial information to the SEC. According to the SEC's XBRL web site, "Data becomes interactive when it is labeled using a computer markup language that can be processed by software for sophisticated viewing and analysis. These computer markup languages use standard sets of definitions, or taxonomies, to enable the automatic extraction and exchange of data. Interactive data taxonomies can be applied — much like bar codes are applied to merchandise — to allow computers to recognize that data and feed it into analytical tools. XBRL (eXtensible Business Reporting Language) is one such language that has been developed specifically for business and financial reporting."

Put differently, financial information is essentially "coded" or "tagged" in a standardized fashion to allow the SEC, to understand it more readily. For example, an accrual, like an executive compensation accrual, is identified and coded as an accrual, along with other types of accruals. In short, XBRL is like a hyper-advanced Twitter hashtag for the financially savvy that allows financial information reported to the SEC to be categorized and sorted quickly and effectively for further analysis.

STANDARDIZED FINANCIAL REPORTING FACILITATES THE AQM INITIATIVE

So how does mandatory financial reporting using XBRL make AQM possible? Through the standardization of reporting, tagging and coding of terms through XBRL, the SEC is able to quantify or "score" the degree to which a company may be engaged in any number of problematic accounting practices. For example, the model analyzes SEC filings to estimate the number and size of discretionary accruals within a company's financial statements. Discretionary accruals are accounting estimates that are inherently subjective and susceptible to abuse by companies attempting to manage earnings. Once anomalous accrual activity is detected, the model then considers other factors that are "warning signs" or "red flags" that a company may be managing its earnings. The SEC has publicly provided limited examples of these factors, which include: the use of "off-balance sheet" financing, changes in auditors, choices of accounting policies and loss of market share to

competitors. Ultimately the AQM quantifies how a company's discretionary accruals and red flags compare to those of other companies within that company's industry peer group. Outliers (those with financial statements that "stick out") in the peer group possess qualities that indicate possible earnings management. As SEC's Dr. Lewis summed up in December 2012: "[AQM] is being designed to provide a set of quantitative analytics that could be used across the SEC to assess the degree to which registrants' financial statements appear anomalous."

It is then up to the SEC to take "the next step" which could vary from company to company. In some cases, a "high score" might warrant a letter from the SEC's Department of Corporate Finance ("Corp Fin") asking for explanations regarding potential problem areas. More dramatically, a "high score," alone or in conjunction with other information, including information provided by a whistleblower, may result in an informal inquiry by the staff of the Enforcement Division, with attendant requests for documents and interviews, or, worse, a formal investigation. Thus, problems for a Company could escalate dramatically with cascading effects, including difficult discussions with the incumbent auditor, and, worst case scenario, a full blown audit committee investigation.

WHAT AQM COULD MEAN FOR PUBLIC COMPANY DIRECTORS AND OFFICERS

A few years ago, AQM may have been viewed no differently than any of the laun-

dry list of items public company officers and directors need to worry about. But arguably in the last 12 months the world has changed: The Division of Enforcement has announced a renewed focus on rooting out accounting fraud, the Task Force the SEC has formed is deploying new strategies to detect and investigate accounting irregularities, and whistleblowers are incentivized to bring allegations of accounting improprieties to the attention of regulators.

So is there a silver bullet to the AQM? How should companies respond to the renewed focus of the SEC on accounting fraud and earnings management issues? There are no right answers to these questions, only perhaps some prudent advice:

GET YOUR XBRL REPORTING RIGHT THE FIRST TIME.

There are many reports that public companies are continuing to make numerous XBRL coding mistakes. It is likely the AQM will not be able to identify an innocent coding mistake. Such mistakes, however, may land a company on the top of SEC's "Needs Further Review" list. Though the audit firms have apparently steered away from giving advice on XBRL, there are numerous experts and boutique firms that can help provide guidance to registrants. Making errors in this area, even if innocent, is simply not an option in this new era.

CONSIDER ALL OF YOUR FINANCIAL DISCLOSURES.

The AQM focusses on identifying outliers. One easy way to become an outlier is to be opaque with disclosures where other companies are transparent. Take a fresh look at your financial disclosures for transparency and comparability across your industry.

LISTEN TO THE SEC'S GUIDANCE.

As we have noted above there are a number of new SEC programs and initiatives focused on detecting financial reporting irregularities. Stay current on SEC activity to avoid surprises.


IT IS NOT JUST THE SEC. XBRL IS AVAILABLE TO THE PUBLIC.

As a greater library of XBRL financial statement data is created, analysts, investors, other government agencies,

media outlets and others will build their own versions of the AQM. Be prepared for greater scrutiny and inquiries from these groups.

BE CONSCIOUS OF RED FLAGS.

For example, a change in auditor is thought to be a significant red flag that might warrant further attention from the SEC.

Finally as we explained above, times have changed and the SEC, upon implementation of the AQM, is ever more likely to knock on your door. Be prepared for interactions with the SEC, in particular the Enforcement Division, that are not in keeping with historical experience. As we advised with the new whistleblower program, be prepared to respond quickly and substantively to any potential SEC inquiry that might have been generated solely by the AQM or one of the many other new tools being employed by the staff. Elevate those inquiries, as appropriate, to the Audit Committee and handle them with the requisite diligence. Further, have your crisis management plan ready, just in case there is a genuine and serious accounting issue that needs attention. Given the potential damage an accounting problem can have on a company's reputation, its investors, and its stock price, have internal and external crisis advisors ready to act if necessary to investigate quickly any potential impropriety. Also have your disclosure lawyers and crisis management advisor ready to communicate with the marketplace in whatever ways are appropriate and at the appropriate time. Indeed, in light of the SEC's renewed focus on accounting improprieties, today, more than ever, a crisis management plan to deal with a potential accounting failures is absolutely essential. 

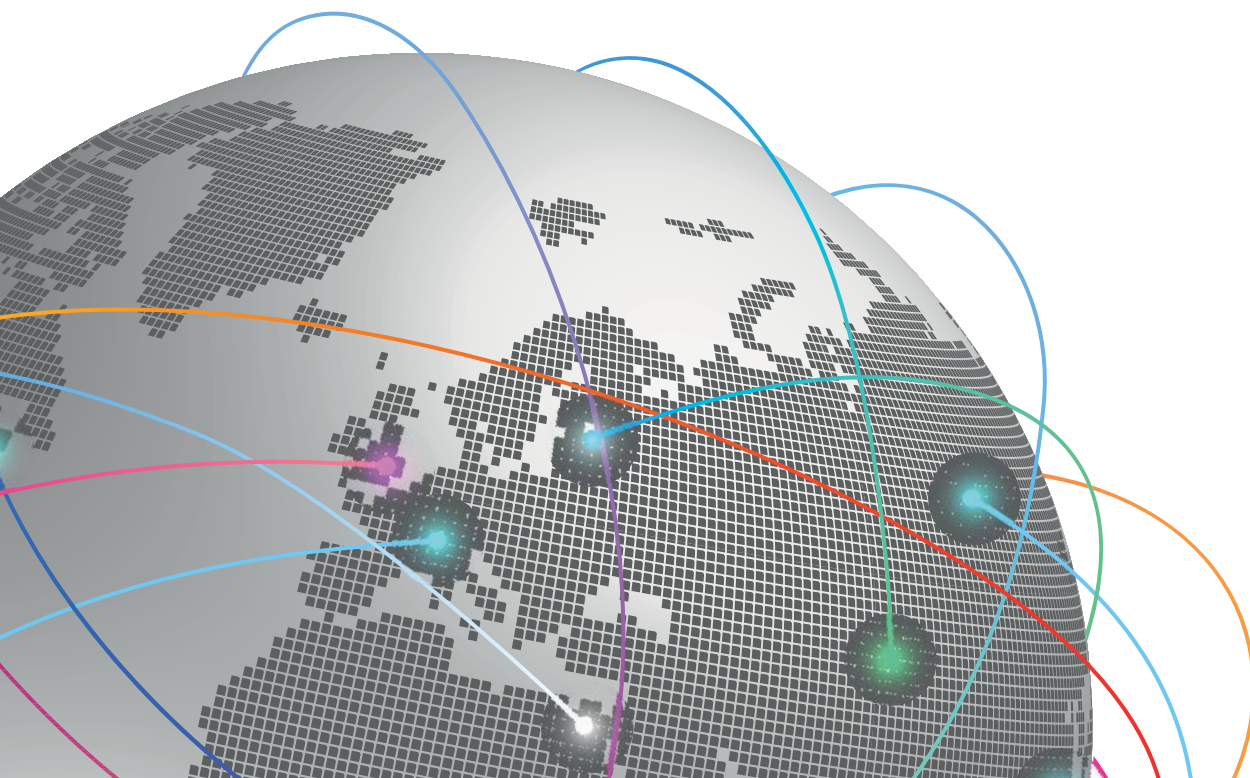
THE GC'S ROLE IN THE DIGITAL REVOLUTION

CORPORATE CAMPAIGNS

Richard Levick

Originally Published on Inside Counsel

Labor/employment practice is no longer
just about contracts and conditions



It's no longer just the danger of bad stories going viral. In the digital age, corporations face a very different and unprecedented threat. Now, an array of hostile forces has integrated strategies, collaborating in multifaceted campaigns to put targeted companies or industries on the defensive, damage reputations and secure significant changes in corporate policy.

They're often referred to as "corporate campaigns" or "global strategic campaigns." The adversaries include labor unions, activist groups, minority shareholders and plaintiffs' lawyers. Their agendas are mutually supportive, such that a lawsuit or an attack on a company's environmental practices can be leveraged to force concessions to union organizers.

If such strategy is formidably protean, the Internet is just the right tool to consolidate this global collaboration. These adversaries use Big Data to gather astounding volumes of information about companies. They organize shareholders online. They launch personal attacks against executives. They don't hope the content goes viral. They make it viral.

Corporate social responsibility is an easy starting point for adversaries to depict responsible actions by companies as mere Band-Aids. When companies like Walmart (a favored target of corporate campaigns) and Target signed on to the Alliance for Bangladesh Worker Safety after April's Rana Plaza building collapse killed 1,100 people, it was a cue for labor groups like the UNI Global Union to counter-attack.

Corporate culpability for Rana Plaza was purportedly implicit as the agreement was a "sham" absent third-party monitors. Yet, if corporations don't sign accords or write checks, that too betrays their moral inadequacy.

UNI – a federation of over 900 affiliated unions and 20 million members in 140 countries – is a prime mover, with significant resources and research capabilities. One 2013 document by its Commerce Sector is rich with data on Walmart's plans to increase its global workforce (and potential new union members). Importantly for corporations that entertain any hope of fighting back, the document is also a digital roadmap to victory, highlighting Walmart's aggressive use of phone and Skype and a strong social media agenda.

Labor is predictably the frontline as organizers work globally, especially on behalf of service workers. Unions draw on multiple potential liabilities, using corporate governance as a cudgel, for instance. Earlier this year, UNI held a public hearing on the Foreign Corrupt Practices Act (FCPA), encouraging whistleblowers to come forward. Meanwhile, the adversary has found many welcome supporters among regulators and public officials, even as activist minions disrupt shareholder meetings, inflaming governance debates or holding transactions hostage.

Because the impact of any single issue may reverberate companywide (i.e. a strike in Brazil could portend other vendettas, perhaps a local environmental problem), the focus of corporate planning must be equally broad in scope. To that end, no one is

better positioned to play a leadership role than the GC. The concomitant business lessons are compelling:

- Corporations can no longer plan for crises that have beginnings, middles, and ends. Corporate campaigns are sustainable ventures and companies must think in terms of a veritable Hundred Years War at every level: What is the long-term viability of a CSR plan? What must IR look like in an era when disruption itself is the activists' goal?
- Corporations cannot fall asleep at the digital wheel, not when the adversary's global agenda is only achievable on the Internet. Companies and industries must match them strategy for strategy.

If the corporate response is to be as necessarily holistic as the attack, there can be no silos, no synapses between IR, HR, etc.

Enterprise risk needs to include 24/7 reviews of online including activities by NGOs, plaintiffs' lawyers, and regulators that suggest linked campaigns. Labor/employment practice is no longer just about contracts and conditions. A new sensibility is required to win the game. **L**

BLOGS *worth following*



THOUGHT LEADERS

Amber Naslund

brasstackthinking.com

Amber Naslund is a coauthor of *The Now Revolution*. The book discusses the impact of the social web and how businesses need to “adapt to the new era of instantaneous business.”

Brian Halligan

hubspot.com/company/management/brian-halligan

HubSpot CEO and Founder.

Chris Brogan

chrisbrogan.com

Chris Brogan is an American author, journalist, marketing consultant, and frequent speaker about social media marketing.

David Meerman Scott

davidmeermanscott.com

David Meerman Scott is an American online marketing strategist, and author of several books on marketing, most notably *The New Rules of Marketing and PR* with over 250,000 copies in print in more than 25 languages.

Guy Kawasaki

guykawasaki.com

Guy Kawasaki is a Silicon Valley venture capitalist, bestselling author, and Apple Fellow. He was one of the Apple employees originally responsible for marketing the Macintosh in 1984.

Jay Baer

jaybaer.com

Jay Baer is coauthor of, “*The Now Revolution: 7 Shifts to Make Your Business Faster, Smarter and More Social.*”

Rachel Botsman

rachelbotsman.com

Rachel Botsman is a social innovator who writes, consults and speaks on the power of collaboration and sharing through network technologies.

Seth Godin

sethgodin.typepad.com

Seth Godin is an American entrepreneur, author and public speaker. Godin popularized the topic of permission marketing.

INDUSTRY BLOGS

Holmes Report

holmesreport.com

A source of news, knowledge, and career information for public relations professionals.

PR Week

prweekus.com

PRWeek is a vital part of the PR and communications industries in the US, providing timely news, reviews, profiles, techniques, and ground-breaking research.

PR Daily News

prdaily.com

PR Daily provides public relations professionals, social media specialists and marketing communicators with a daily news feed.

BUSINESS RELATED

FastCompany

fastcompany.com

Fast Company is the world’s leading progressive business media brand, with a unique editorial focus on business, design, and technology.

Forbes

forbes.com

Forbes is a leading source for reliable business news and financial information for the World’s vvbusiness leaders.

Mashable

mashable.com

Social Media news blog covering cool new websites and social networks.

COMMUNICATING TRUST