

- 2...ACC Speaks with General Counsel and Chief Legal Officers about Their Changing Roles
- 4...Be Empowered and Protected
- 4...ACC News
- 5...A Brief Survey of Current and Future Developments in Privacy, Data Protection and Cyber Security Law

- 7...Patent Trolls: The Reason Every Business Should Care About Patent Litigation Reform
- 9...Effectively Managing Federal Investigations
- 10...Welcome New Members!
- 10...Board Members and Contacts

FOCUS

President's Message

Mark Rogers

Many thanks to Snell & Wilmer, Gallagher & Kennedy, and Altep for the articles in this quarterly newsletter! Thanks, too, to Altep for their sponsorship of the Chapter as this year's Newsletter Underwriter.

It is hard to believe that we are already well into our 2013 – 2014 year, but the year is underway and programs are well attended. Even though we have increased the number of programs, **programs are still selling out**. In particular, the members only programs we offer to you at no charge on the first Thursday of the month and what we call our "Middle Wednesday" programs (often, but not always, in the week between our first Thursday and our third Tuesday meetings) often sell out very quickly, sometimes within hours of the registration opening within Eventbrite. We maintain a wait list, so please add your name to the list if an event you'd like to attend is sold out. It is worth the trouble — we do sometimes receive cancellations. **Still, if you see an event announcement and want to attend, please register right away.**

In addition to adding CLE programs this year, we added a number of purely social events to our calendar, including a few family friendly events. Please watch closely for email announcements about those — as with our CLE sessions, there is a lot of interest in these, so the available tickets tend to go quickly.

I wrote last quarter about the Third Annual Arizona Corporate Counsel Awards (congratulations again to the finalists and winners) in January. I mention it again this quarter because *it is never too early to start thinking about nominations for the Fourth Annual Arizona Corporate Counsel Awards in January 2015* — think about nominations, budget to attend the event and come to celebrate the work done by your teammates and colleagues in the in-house bar. I'm going to make a special plea here for patent lawyers in-house. Please, help us identify and celebrate their work.

As the in-house bar in Arizona has grown and as our Chapter has grown over the past several years, one of the things our Chapter (and ACC) can feel good about is how long people maintain their membership. I've had occasion recently to look at Chapter membership and the date members joined ACC — a handful of our members have been ACC members since before the formation of the Arizona Chapter! Here are a few of the findings:

- More than 50 have been members for more than 10 years
- Just over 100 Arizona Chapter members joined ACC 2004 – 2008
- From 2009 through June 2013, we added more than 220 members to the ranks (more than doubling the rate of growth in the prior five-year period)

We are looking at ways to celebrate our long-standing members and thank them for their continued membership. If you have any ideas on this topic, please email them to the Chapter.

While we are very pleased with the growth of the Arizona Chapter, it is always important to remember that the point of growth is to continue improving and adding to the services we provide to you, our members — more and better programs, unique benefits for members, social and networking events with peers, etc. If you have ideas for how we might continue to evolve, please email those ideas to the Chapter, too.

I'm still looking forward to the day that I can announce hitting the 400-member milestone. Please, continue to recommend membership to other eligible in-house counsel. Talk to them about the benefits of membership — you are all capable of putting on a persuasive case for membership.

As always, thank you for your attendance at meetings, and thank you for your interest in ACC and the Arizona Chapter.

I hope to see you at an upcoming meeting soon!

ACC Speaks with General Counsel and Chief Legal Officers about Their Changing Roles

Justin A. Connor, ACC Senior Counsel & Director of CLO Services

ACC has released several recent publications focusing attention on the areas that matter most to general counsel (GC) and chief legal officers (CLOs): benchmarking, knowledge sharing, best practices and thought leadership on the challenges of leading the legal department in today's complex corporate environment. In December 2013, ACC published *Skills for the 21st Century General Counsel*, a report forming part of the ACC Executive Series, in cooperation with Georgetown Law's *Center for the Study of the Legal Profession*. In order to prepare the report, ACC had extended interviews with 28 thought leaders in the in-house legal profession – including current and past general counsel of leading companies, independent directors of major companies, chief executive officers (CEO), executive recruiters and others. In cooperation with the *National Association of Corporate Directors* (NACD), ACC also surveyed 78 corporate directors. Finally, ACC surveyed 689 CLOs and GCs within its membership base to gather the following report findings.

How ACC Serves CLO Members

Effectively serving GCs and CLOs is one of ACC's key strategies identified in its Strategic Plan for 2013-2018. In line with its strategy, both the "Skills for the 21st Century General Counsel" report and the annual CLO Survey support members by providing benchmarking data, comparison of key metrics and an overall sense of the most important issues facing CLOs today.

ACC, through its *CLO Services* department, aims to encourage further engagement by CLOs in numerous ways, from participating in the *CLO Club* events, serving as faculty at the *Annual Meeting*, authoring or co-authoring an *article or resource* for in-house counsel and serving on ACC Advisory Boards to attending *CLO Roundtables* to benchmark with their peers, being profiled for the *CLO Executive Bulletin* and attending CLO events organized by *chapters*.

ACC is also reviewing the executive education programs with an eye toward launching the ACC Executive Leadership Institute to develop exciting new programs for law department leaders and heighten existing efforts to increase CLO engagement. Ensuring that our association and its activities always remain relevant, practical and immediately useful to our members and their law departments is one of ACC's main priorities.

To that end, CLO Services is pleased to offer the following executive summary of two recently released reports: *Skills for the 21st Century General Counsel* report and the ACC 2014 *CLO Survey*, both of which directly address the dynamic role and high expectations of today's general counsel.

Leading the Legal Department

Quote from a former GC:

"Everyone at the top wears multiple hats. You need to deeply understand the business and where it is headed, so your GC hat doesn't go out the window, but you simply put on more hats. Many of the business people do as well. You want them to wear a compliance hat and a risk hat, for example, in addition to a business hat. So you become much more integrated into that world, but it definitely requires more training and more understanding of the business."

The most important job of a GC and CLO is still chief provider of legal advice and manager of the legal department. About 84 percent of GCs report providing legal advice and managing legal matters for the company as one of the top ways they provide value to their organizations. Although nearly three-quarters (74 percent) of corporate directors rated these more traditional functions in the top three contributors to value, they were more likely to see value in other activities. Directors were much more likely, for instance, to view the compliance function as a source of value than GCs themselves (54 percent vs. 34 percent).

And while managing legal expenditures was lower on the list of value-add activities (approximately 10 percent of both directors and GCs rated this in their top three), more experienced GCs were much more likely to report that they add value through this activity (19 percent of GCs with more than 10 years of experience in prior GC roles).

As legal departments cope with increasing regulation, complexity and globalization, without corresponding increases in resources, effective legal department management is more important than ever. As these trends continue, future GCs will first need to have an excellent understanding of the business, and its sources of cash flow, risk and strategic priorities. Using this information, GCs must then be able to creatively address resource constraints by continuously re-evaluating the way they staff legal matters, use outside counsel and manage processes. They will need to be adept at managing a team of lawyers who are sometimes globally dispersed, even in smaller companies.

We predict more splitting of the GC role, so that a legal chief operating officer may be more focused on management of the department, while the GC/CLO focuses more on counseling and strategic activities, especially as legal department management needs increase.

GC as Counselor in Chief

Quote from an executive recruiter specializing in general counsel searches:

"I can't tell you how many times the first words out of the CEO's mouth are: 'I need a business partner.' Sometimes, that's code for: 'I currently have a GC who may be a good lawyer, but he or she is not astute regarding the business issues that our business is facing.' That comes up constantly. They don't want someone who has got an ivory tower mentality, and a lot of lawyers do."

continued on page 3

continued from page 2

The second key area where GCs provide value to their organizations is through counseling the CEO and board of directors. Approximately half of GCs and directors cited counseling the CEO as one of the top three value-drivers. Although fewer GCs (20 percent) cited counseling the board of directors as a top source of value, a much higher percentage of board members (38 percent) view this activity as a significant source of GC value, suggesting that many GCs do not fully appreciate the positive impact of their contributions to their organization's board.

The counseling role goes beyond simply providing legal counsel; the GC also serves as a trusted advisor to the CEO and the board. GCs must perform a delicate balancing act between being trusted and active members of the management team (i.e., having a "seat at the table") and maintaining their independence. To serve in this role, future GCs will need to possess the managerial courage to say "no," even when it is unpopular.

To do this effectively, they will need to have excellent communication skills and emotional intelligence to ensure they are constructive in their assessment of risk and rewards in a business context. They also must build credibility and respect with their executive peers, which are influenced by the degree to which they demonstrate the third essential skill — being a strategist.

GC as Strategist

Quote from a current general counsel with 11 years in the GC role:

"I think the biggest surprise to me was the extent to which technical legal expertise is really not that important. ... I think you have to expect that your general counsel is going to be a very good lawyer, but there are a lot of people who are very, very good lawyers but, in my opinion, wouldn't make great general counsel. That's the base level, and I think that you should be able to take that for granted. The things that make you a great general counsel have very little to do with technical legal expertise."

Perhaps the most striking finding of this study is the growing importance of the GC role as a strategic thinker. Looking ahead five to 10 years from now, both GCs and corporate directors view strategic input as becoming a larger source of added value. However, there is a disconnect between GCs and directors when it comes to the contribution of strategic input: GCs are much more likely than directors to rate the GC's role in providing strategic input into business decisions as being in the top three sources of added value, both now and in the future. This difference in opinion may be especially important given a distinction directors make when evaluating the performance of their GCs. According to directors, the highest performing GCs add value by contributing strategic advice.

With strategic input increasing in prominence and necessity, future GCs would be wise to develop strategic-thinking skills. They need to be comfortable with risk and helping their business colleagues decide which risks are reasonable and which are not. On the other hand, GCs cannot focus wholly on risks and constraints, as they also need to define and embrace opportunities, especially conversations about strategic choices — both as lawyers and as general managers who are trained in the law.

A broad worldview, an ability to network and generate ideas with people from diverse perspectives and ability to focus on the longer-term impact of decisions is equally important as understanding the risks and opportunities facing one's company.

As previously noted, GCs increasingly play a more meaningful role in executive and boardroom conversations as they move from traditional legal advisors to corporate strategists. GCs may help their organizations adapt to faster-moving environments by utilizing their mediation skills and insight across the business spectrum to bring diverse perspectives together and solve business challenges.

In the role of integrator, GCs can help drive organizational innovation and renewal. Integrator GCs can broker disparate pieces of information across

organizational silos, while also assisting the executive team in setting up a culture where measured risk in the pursuit of new ideas is nurtured.

The full report explains the ACC's findings and details the evolution of GCs from legal advisor to counselor to strategist. Particularly, the ACC's research seeks to capture the current state of the role of GCs, understand how and where the role appears to be evolving and identify skills and competencies required for GCs to be successful in the future.

Future generations of GCs will find a job that is broad-ranging, impactful, innovative and increasingly global in scope — a rewarding prospect for those prepared to meet its diverse challenges.

The ACC CLO 2014 Survey

Quote from Patricia R. Hatler, Executive Vice President, Chief Legal and Governance Officer, Nationwide Insurance:

"I once worked for a CEO who said the only reason he could sleep at night was a strong culture of ethics and compliance at the company. The more experience I have, the more I see how right he was. In today's environment, a compliance mindset has to be 'in the water.' It has to be everyone's job."

Highly regulated businesses are even more highly regulated today. There are more regulators, and they are more active. Companies have to devote resources to staying on top of those regulatory expectations and building effective communications with the regulators."

To understand the driving forces behind the evolving role of the CLO and of corporate legal departments, ACC reached out to 9,600 individuals. The CLO 2014 Survey results reflect response data from more than 1,200 individuals in 41 countries who serve as the organization's CLO or GC. From roles and responsibilities to salaries, skills and work environments, the study explored a broad range of topics and is the most comprehensive global study of its kind to date.

continued on page 8

Be Empowered and Protected

Face your challenges better with help from two ACC Alliance partners who can help you prepare for whatever may come. Look at these two unique offers:

- “*Knowledge is power.*” That’s what 16th Century English philosopher and jurist, Sir Francis Bacon, famously stated. How would learning the settlement secrets of elite negotiators empower you? ACC Alliance partner, **Agency for Dispute Resolution**, is kicking off 2014 with an event exclusively for you, our members.

They are bringing their top-caliber negotiation training developed and taught by core faculty of the #1 ranked Straus Institute to a broader base, at a deeply discounted introductory rate. To find out more, please visit www.NegotiationisPower.com. (Use promo code BIRD4 to save \$125 if you register before February 28.) If nothing else, you’ll receive a free copy of their latest whitepaper, “*The 5 POWER Plays to Victory in High-Stakes Negotiations.*”

- Now, imagine that you are investigated for the failure to provide legal advice even though no one sought your counsel. Is your silence a viable defense to liability or could a court find that you had a duty to speak up? Our ACC Alliance partner, *Chubb*, can help. **Learn more** from Chubb about malpractice issues unique to in-house counsel.

Find out more about all of the Alliance partners at www.acc.com/alliance.

ACC News

ACC Annual Meeting: Register by April 2 and Save

Save \$200 off the regular registration rate for the ACC Annual Meeting in New Orleans (Oct 28–31) if you reserve your spot by April 2. This meeting presents an unmatched combination of timely and relevant topics, peer-to-peer networking, and a year’s worth of CLE/CPD credits. View the complete program schedule and register at am.acc.com.

New Career? Attend Corporate Counsel University®

Designed specifically for lawyers with less than five years of in-house experience or those who want to enhance their basic practice skills, the ACC Corporate Counsel University® (June 1–3, Minneapolis, MN) helps you jumpstart your in-house career. Programs cover important topics such as contracts, compliance and employment and more. For more information, visit ccu.acc.com.

Compliance Training to Protect Your Company

The ACC Compliance & Ethics Training program is back by popular demand. Join your peers in Austin from April 7–8 for this interactive CLE/CPD program. Program topics cover compliance essentials critical to your practice, including: Compliance Investigations, Attorney-Client Privilege in the Compliance Context, Data Privacy and Cross-Border Transfer of Data and more. Learn more and register at www.acc.com/ce.

Emerging Global Trends for Corporate Counsel

Mark your calendar for the newest educational program from ACC: Emerging Global Trends for Corporate Counsel (June 19–20, Toronto, Ontario). Dive deep into emerging global trends and their implications for general counsel in Canada and around the world. Get up to speed on recent developments in global anticorruption regulations, corporate governance, cross-border privilege and more. Advance registration rates are available through April 24. Learn more at www.acc.com/egt.

Executive Workshop on Driving Value in Legal Spending

Are you getting the most out of your law firm relationships? Attend the ACC Legal Service Management Workshop (May 6–7, St Louis, MO) to develop skills in implementing value-based fee structures and management skills. Secure your spot today at www.acc.com/legalservicemanagement.

Mind your Business

In today’s environment, you can’t operate in a legal silo. It’s imperative to understand the business operations of your company in order to make effective legal decisions. Attend targeted courses offered by ACC and the Boston University School of Management to learn critical business disciplines essential to your in-house practice.

Upcoming Programs include:

- Advance Mini MBA for In-house Counsel (April 2–4)
- Mini MBA for In-house Counsel (May 6–8, Los Angeles; June 11–13; September 17–19; and December 3–5)
- Project Management for the In-house Law Department (September 29–30)
- Risk Management & In-house Counsel (October 7–9)

All programs take place in Boston unless otherwise noted. Learn more and register at www.acc.com/businessedu.

Celebrating Pro Bono and Diversity

Have you or someone you know of made great strides in promoting diversity in the legal profession or providing outstanding pro bono legal services? Submit your nominations today for the ACC 2014 Matthew J. Whitehead, II Diversity Award and Corporate Pro Bono Award to celebrate the great achievements! Deadline for nomination is May 30. Learn more at www.acc.com/diversityaward, and www.acc.com/probonoaward.

Save Time and Money with ACC Contracts Portal

If you haven’t yet, be sure to check out the ACC Contracts Portal and take advantage of the valuable tools and resources it offers. Use the Portal to draft and benchmark contracts, prepare yourself to enter into tough contract negotiations, and effectively manage your contracts. Learn more at www.acc.com/contracts.

A Brief Survey of Current and Future Developments in Privacy, Data Protection and Cyber Security Law

By Patrick X. Fowler, Partner, Snell & Wilmer LLP

The challenges confronting corporate counsel regarding privacy, data protection and cyber security have never been more daunting: dealing with the threat of increasingly sophisticated cybercriminals, responding to data breach incidents, keeping up with a myriad of evolving national and international laws, regulations and industry standards, all while wondering if your data has been targeted by a government surveillance program.

And they're not letting up in 2014. New online privacy laws in California already went into effect on January 1. In February, the federal government is expected to publish a new "cybersecurity framework" for critical infrastructure in the U.S., and that framework, like it or not, may well set a future *de facto* standard of care for establishing liability. In addition, in response to the massive retail customer data breach that occurred late last year, Congress may finally pass a national personal data privacy and security law.

I. Data Breaches, Cyber-Crimes and Data Center Outages: By the Numbers

A. The High Cost of Fending Off the Barbarians at the Gate, as well as Those Already Inside the Walls

When it comes to data breaches, no one is immune. Organizations of all shape and sizes, from government agencies to internet startups, retail brands to respected financial institutions have reported major data breaches in the past year. According to figures kept by the Open Security Foundation, there were 1,390 data breach events reported in 2013.¹ One study found that 41% of US data breaches were due to malicious or criminal attacks, with 33% caused by human factors (negligence) and 26% from system failures or glitches.²

Smaller companies no longer operate under the hackers' radar. In 2012, 50% of all targeted cyber-attacks were aimed at businesses with fewer than 2,500 employees, and *the largest growth area for targeted*

*attacks was businesses with fewer than 250 employees: 31% of all attacks targeted them.*³ Applying the time-tested strategy of following the path of least resistance, attackers thwarted by a large company's defenses will try instead to breach the lesser defenses of a small business that has a relationship with (and perhaps easier electronic access to) the attacker's ultimate target.

Perhaps more troubling is how long it took to spot the breaches. Verizon noted in its 2013 study that *66% of breaches took months or years to discover.*⁴ The median number of days between the breach and its discovery was 243 days, or about eight months (which was actually a marked improvement over the prior year).⁵ And when the breaches were finally detected, 63% of the discoveries were made by someone *outside the organization.*⁶

The average organizational cost of a data breach was \$5.4 million.⁷ This included detection and escalation costs (\$395,000), notification costs (\$565,000), post-breach costs (\$1.4 million) and lost business costs (\$3.03 million).⁸ When viewed in a "per capita" context, the average per record cost of a data breach in 2012 was \$194, as compared to \$188 per record in 2011.⁹

B. Cyber-Crimes Apparently Do Pay

While cyber-crimes comprise just one slice of the data breach pie, it is a huge portion. The annual cost of cyber-crime and cyber-espionage to the U.S. is as much as \$100 billion.¹⁰ The reported average cost to resolve a single successful cyber-attack (one that results in the infiltration of a company's core networks or enterprise systems) ranges from \$300,000¹¹ to more than \$1 million,¹² with an average annualized cost of cyber-crimes to be more than \$11.5 million.¹³ The average time to resolve a cyber-attack was 32 days in 2012 (as opposed to 24 days in 2011).¹⁴ However, malicious insider attacks can take more than 65 days to contain.¹⁵ Moreover, with the recent emergence of so-called "ransomware" such as CryptoLocker (malware that encrypts user data and holds it for ransom¹⁶), the threat of cyber-crime is not likely to diminish.

C. When the Power Goes Out: The Cost of Data Center Outages

Aside from data breaches and cyber-crimes, companies that rely on remote data centers for web hosting, data processing and/or information storage (i.e., cloud computing) can suffer significant losses when the data center goes off-line, even temporarily. In 2013, the average cost of an unplanned data center outage was reported to be slightly more than \$7,900 per minute, a 41% increase from 2010. The average reported outage length was 86 minutes, resulting in an average cost per outage of approximately \$690,000 (compared to 97 minutes and \$505,000 in 2010).¹⁸

¹ Open Security Foundation / DataLossDB.org <http://datalossdb.org/statistics>

² Ponemon Institute "2013 Cost of Data Breach Study: Global Analysis", May 2013

³ Symantec Corporation, "Internet Security Threat Report", Vol. 18, April 2013 http://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_v18_2012_21291018.en-us.pdf

⁴ Verizon, 2013 Data Breach Investigations Report

⁵ Mandiant, M-Trends 2013: Attack the Security Gap, March 2013 <https://www.mandiant.com/resources/mandiant-reports/>

⁶ Id.

⁷ Ponemon Institute "2013 Cost of Data Breach Study: Global Analysis", May 2013

⁸ Id.

⁹ Id.

¹⁰ Center for Strategic and International Studies, "The Economic Impact of Cybercrime and Cyber Espionage." July 2013 <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf>

¹¹ IBM X-Force 2012 Mid-Year Trend and Risk Report, September 2012

¹² Ponemon Institute "2013 Cost of Cyber Crime Study: United States", October 2013

¹³ Id.

¹⁴ Id.

¹⁵ Id.

¹⁶ <http://www.pcworld.com/article/2084002/how-to-rescue-your-pc-from-ransomware.html>

¹⁷ Ponemon Institute, 2013 Study on Data Center Outages, September 2013

¹⁸ Id.

continued on page 6

II. A Patchwork of Privacy and Data Breach Notification Laws and Rules

The lack of a comprehensive, uniform set of privacy and data protection laws has been an on-going source of frustration for corporate counsel. The U.S. does not have a national privacy and data protection law — at least not yet. Instead, 46 states, along with several territories, have enacted non-uniform laws that provide various types of protection for personal information. There also exists a hodge-podge of federal laws protecting particular types of records (e.g., health records, school records, financial records).

A. California Continues to Expand the Universe of Privacy Laws

Already in 2014, California has added two new laws to its online privacy protection scheme.¹⁹ Effective January 1, website and mobile application operators must update their privacy policies to disclose how the site responds to so-called “Do Not Track” signals designed to tell websites or mobile applications that the user does not want the website operator to track his or her visit to the site. The law applies to all companies that collect tracking information from California residents, and accordingly applies to companies that do business in California and track California residents, even if the company does not have a physical presence in California. (Notably, California has not mandated that website and mobile application operators actually honor a “Do Not Track” signal — only that the user be provided with a disclosure about how the website will respond to such signal.)

The other addition to California’s privacy policy requirements requires website operators to disclose whether third parties may collect personally identifiable information about the user’s online activities over time and across different websites.

B. Congress Mulls Several National Privacy and Data Protection Bills

In response to the massive security breach announced by Target late last year, at least

three different data protection and breach notification bills have been introduced in the Senate.²⁰ One such proposal, the Personal Data Privacy and Protection Act of 2014, re-introduced by Sen. Patrick Leahy (D-Vt) for the fifth time, would nationalize data breach notification laws and impose new data protection requirements on businesses that hold personal data on more than 10,000 individuals. Similar bills have been introduced many times in past sessions without success. However, given the confluence of several recent highly publicized events involving aspects of privacy, data breach and cybersecurity and the alleged lack of consumer protection, the chance for passage of some reactionary federal legislation in this area is greater than in the past several years.

C. The Federal Government’s Proposed Cybersecurity Framework for Critical Infrastructure

In February 2013, President Obama issued Executive Order 13636 titled “Improving Critical Infrastructure Cybersecurity”²¹ It contained several key features: (1) requiring government entities to share cyber threat information with the private sector, (2) the impact of cybersecurity activities on privacy and civil liberties must be assessed, and most importantly, (3) the creation of a comprehensive, but voluntary cybersecurity framework for companies involved in critical infrastructure to adopt.

Critical infrastructures have been defined by the federal government as including 16 different “sectors.” These are chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, material and waste, transportation systems, water and wastewater systems.

The National Institute of Standards and Technology (NIST) (part of the Department of Commerce) was charged with developing this framework within a year. NIST conducted several workshops across the country and before it released the preliminary framework last summer²³, it consulted

with more than 3,000 interested parties on best practices for securing IT infrastructure. The final version is expected to be released sometime around February 2014.

Suffice it to say that the potential impact of the framework, once issued, is significant. Given that level of broad input and degree of consultation in creating the framework, at least one commentator has observed that once finalized and released, the framework will be recognized as an industry standard.²⁴

While it is intended to be — at least initially — a voluntary program for owners and operators of critical infrastructure, the federal government is already taking steps to encourage adoption of the framework, such as considering changes to the federal acquisition regulations. Additional incentives are being contemplated, such as those involving insurance, possible liability limitations for companies that adopt it, and making adoption a condition for receipt of federal grants. Consequently, companies that work within the critical infrastructure sectors would be wise to review the framework and evaluate their ability to adjust their cyber security policies and practices to meet it.

III. Conclusion

The technical, societal and legal developments in the realm of privacy, data protection and cybersecurity continue to unfold in remarkable and unpredictable ways. Given the pace and significance of these changes, it is essential for companies and their lawyers to keep a close eye on them.

¹⁹http://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB370&search_key-words=

²⁰<http://www.bankinfosecurity.com/breach-notice-bills-pile-up-in-senate-a-6398> (January 15, 2014)

²¹<http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf> 0

²² <http://www.dhs.gov/critical-infrastructure-sectors>

²³<http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf>

²⁴<http://www.informationweek.com/government/cybersecurity/nist-cybersecurity-framework-dont-underestimate-it/d/d-id/1112978> (December 9, 2013)

Patent Trolls: The Reason Every Business Should Care About Patent Litigation Reform

By Donna H. Catalfo, Shareholder, Intellectual Property, Gallagher & Kennedy, P.A.

Patent trolls are companies established solely for generating revenue through threatened and actual patent infringement litigation. They do not make or sell any products or services. Their business model is to use bad patents issued in the '80s and '90s — primarily broad business method and software patents that cover large abstract ideas — to extort settlement payments.

The past few years have seen not only an explosion in patent troll litigation,²⁵ but also a shift in the demographics of that litigation, with trolls targeting retailers and end-users of products and services accused of infringement, rather than the technology company that manufactured them. As a result, more and more small-to-mid-sized businesses have found themselves in the middle of these disputes. For example, of all patent lawsuits filed from January through November 2012, 55% of the defendants made \$10 million or less in annual revenue compared to 16% in non-troll patent litigation.²⁶ The types of products targeted by trolls are often in wide use, such as credit card terminals, store locators on websites, and systems for sending text messages that contain a hyperlink to your website. As a result, no business is immune.²⁷

Patent troll litigation has a significant negative impact on any given business and the economy as a whole. One estimate found that it cost the U.S. economy \$29 billion in 2011 alone.²⁸ The amounts paid in settlement simply line the pockets of the patent trolls and their contingency-fee attorneys. It is not reinvested into research and development because patent trolls, by their very nature, don't research or develop anything. These forced settle-

ments take resources away from legitimate businesses that would have invested in expansion or research and development.

Defendants choose to pay settlements, despite what are viewed as frivolous claims, because the cost of defense in these cases can be onerous²⁹ and because our current enforcement system is structured such that patent infringement defendants bear a disproportionate share of the overall costs. The standard for asserting patent infringement is relatively low, and that assertion is all a troll needs to create leverage for settlement. It is defendants that bear the burden of investigating and *proving* non-infringement and invalidity defenses. Defendants can sometimes reduce costs by participating in joint defense groups, but not every defendant uses or sells the identical product. Defendants must still invest significant resources to analyze the facts of their individual case to be sure that claim construction, invalidity and non-infringement positions advanced by the group are helpful, and not detrimental, to that defendant.

Furthermore, discovery costs are one-sided. Patent trolls are typically shell companies that have few records, and therefore, incur little in the way of costs to respond to discovery. Conversely, the patent troll will seek the full scope of broad discovery currently allowed by our procedural rules related to the purchase, use and sale of the accused product, as well as sensitive financial records that allow the patent troll to assess its "damages." In addition to out-of-pocket litigation costs, defendants who have actual businesses to run face considerable lost time and business disruption as employees are tasked

with gathering documents, providing information and even testifying. For patent trolls, litigation is standard operation.

Defendants must invest substantial sums in attorneys' fees and expert fees to defend the case. Importantly, even if the defendant prevails, these fees are rarely recovered under the existing patent law framework. Patent trolls, on the other hand, retain counsel on a contingency basis. Patent trolls count on this asymmetrical allocation of cost to extract settlement payments in an amount less than the cost of defense, but still significant to the defendant's bottom line. Because of the high cost, many businesses opt to pay.

We Must Curb Abusive Patent Litigation by Leveling the Playing Field

State and federal governments are taking measures to respond to this escalating problem. The measure likely to have the greatest impact is federal legislation. Several different members of Congress have introduced a variety of bills aimed at curbing abusive patent litigation. The most noteworthy bill to date is H.R. 3309, the "Innovation Act." The House of Representatives passed the bill on December 5, 2013, and it is currently before the Senate Judiciary Committee. The current version of the bill provides as follows:

- Courts will be required to award the prevailing party costs and fees "unless the court finds that the position of the nonprevailing party . . . was substantially justified in law and fact" or "special circumstances . . . make an award unjust." Under the existing standard, an award of attorneys' fees is discre-

²⁵Patent troll lawsuits rose from 29% of all infringement suits in 2010 to 62% of all infringement suits in 2012. Chien, Colleen V., *Patent Assertion Entities, Presentation to the DOJ/FTC hearing on PAEs*. Washington, D.C., December 10, 2012.

²⁶Chien, Patent Assertion Entities, *Presentation to the DOJ/FTC hearing on PAEs*.

²⁷It has been estimated that patent trolls threatened suit against as many as 100,000 companies in 2012 alone. Chien, *Patent Assertion Entities, Presentation to the DOJ/FTC hearing on PAEs*.

²⁸Bessen, James E. and Michael J. Meurer. "The Direct Costs from NPE Disputes." *Boston University School of Law, Law and Economics Research Paper No. 12-34*, June 28, 2012.

²⁹In 2013, the median cost to defend patent infringement cases brought by patent trolls ranged from \$300,000 to \$2.5 million through the end of discovery, and ranged from \$600,000 to \$4 million through resolution. AIPLA, *Report of the Economic Survey 2013*.

continued on page 8

continued from page 7

tionary and permitted only in “exceptional cases.” The new law would shift significant risk and costs to the patent troll, providing a disincentive for filing frivolous cases.

- In the complaint, the plaintiff will be required to state with specificity how the accused product infringes. This increases the burden and cost on the plaintiff at the pleading stage to state a sufficient case of infringement, preventing patent trolls from skating by with form documents and barebones complaints.
- The plaintiff will be required to disclose ownership information including assignees, parent entities and any other entities with rights or financial interests in the patent. In certain situations, a prevailing defendant could recover its costs and fees from these entities if the named plaintiff is unable to pay.
- Under certain conditions, manufacturers would be permitted to intervene in a patent suit brought against customers, and the suit would be stayed as to the customer while the plaintiff and manufacturer litigate the merits.
- Discovery prior to claim construction³⁰ would be limited.

- Plaintiffs could not rely on demand letters to establish willful infringement unless the letter sets forth infringement allegations with particularity. The typical form letters from patent trolls would no longer suffice.

In general, businesses support passage of the Innovation Act and feel that it is a step in the right direction. However, some startups and small businesses are concerned that the law will make it harder for small inventors with valid patents and infringement claims to protect their rights.³¹ Additionally, some commentators view legislation as unnecessary given the Federal Circuit’s recent decision in *Kilopass Technology, Inc. v. Sidesense Corp.*, ___ F.3d ___ (Fed. Cir. 2013) (O’Malley, J.). There, the court vacated the denial of attorneys’ fees and emphasized that trial courts have set too high a bar for establishing a case is “exceptional.” But *Kilopass* did not involve a patent troll, and the opinion does not address how the fact that a non-prevailing party is a patent troll should factor into the analysis, if at all. The decision touches on only a single issue, recovery of fees, and does not go far enough.

Proactive Engagement Needed

Until the risks and costs of patent litigation are balanced, patent trolls have no incentive to stop using the current system for their own gain. There is significant money to be made — at great cost to innovation. Interested parties should keep pressure on Congress to act. Many trade associations, including the National Retail Federation, National Restaurant Association and Consumer Electronics Association, have already come out in support of the Innovation Act. You can make sure your trade association is monitoring the legislation and voicing an opinion on pending legislation. Additionally, Arizonans can contact the office of Arizona Attorney General Tom Horne and voice support for legislative reform. Many state attorneys general have already taken state-level action against patent trolls in an effort to protect local businesses. Arizona Attorney General Tom Horne demonstrated his support for reform when he signed a letter to the Federal Trade Commission voicing support for that agency’s investigation into abusive patent litigation. Perhaps he could be persuaded to do even more.

³⁰Claim construction is the process by which the parties brief and argue, and the court then construes, the meaning and scope of key terms in the patent claims. Usually this must take place before there can be any ruling on the merits.

³¹Fox Business, *Innovation Act Divides Startups, Small Businesses*, Dec. 5, 2013 at <http://smallbusiness.foxbusiness.com/entrepreneurs/2013/12/05/innovation-act-divides-startups-small-businesses/>.

³²<http://apps.americanbar.org/buslaw/blt/2009-09-10/joshi.shtml>

continued from page 3

Specifically, the annual report discusses CLOs’ prioritization of business issues, adoption of practices that drive greater value for law departments and concerns for the coming year. New this year is a comparative analysis of the data from the 2013 and 2014 survey results, thereby addressing current trends facing law departments.

Increasingly it falls upon CLOs to identify issues related to ethics and compli-

ance as their influence has grown within their companies. Therefore, it is not surprising this ranked as a top concern for 2014. Minimizing compliance risks facing organizational liability and expanding into new markets requires a high level of knowledge and experience. From global expansion to the rapid adoption of new technology, businesses are increasingly facing new challenges and uncharted waters.

Regulatory or government changes and information privacy ranked second and third respectively as pressing issues keeping CLOs up at night now and in the year ahead. Taking note of GCs’ and CLOs’ current and future concerns not only plays an important role when organizations seek to expand into new areas or new markets, but also in terms of handling levels of complexity that require a combination of business and legal expertise.

Effectively Managing Federal Investigations

By Altep

When a federal regulatory agency comes knocking, Altep can help you minimize your exposure — and the impact on normal operations — with a comprehensive and efficient response plan.

After a decade of high-profile financial scandals, consumers, employees, regulators and the media have all become hyper-sensitive to corporate malfeasance. The mere suggestion of impropriety can quickly result in an investigation, and both the scope and frequency of regulatory activity have expanded.

Passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 provided a framework for “sweeping overhaul of the United States financial regulatory system, a transformation on a scale not seen since the reforms that followed the Great Depression.”ⁱ

The ability to mount an appropriate response to an investigation — whether internal or federal in nature — is becoming increasingly critical for those charged with corporate governance. Complex information and technology infrastructures require a sophisticated approach to e-Discovery, and heightened scrutiny from both the public and government agencies necessitates a response plan that is both inward and outward facing. Defining and implementing such a plan poses significant challenges for the corporation and its inside and outside counsel; however, with proactive planning, appropriate technology, and a well-positioned message, corporations can successfully implement cross-functional teams and protocols that will support an effective response and minimize the long- and short-term impact of any investigation.

Developing an Effective Discovery Management Program

Where discovery and compliance are concerned, “appropriate protocols” are those that are repeatable, defensible and effective. Each aspect of the corporation’s discovery management

effort, from legal holds to collection to data analysis should be thoroughly planned and documented. Additionally, as recent cases (Broadcom, Stanfordⁱⁱ and others) have illustrated, standardized protocols which clearly address the Upjohn warning are especially critical. Finally, the methods employed for data collection, processing, analysis, review and production must be appropriately thorough, and the chain of custody must be meticulously maintained throughout the entire discovery lifecycle.

In order to be effective, the discovery management program must allow the organization to locate the needed information in a manner and at a pace that minimizes financial exposure and risk of sanctions, with sufficient objectivity to prevent public and governmental mistrust of processes and activities, and at a cost that is predictable and manageable.

In the event of an internal investigation, ensure thoroughness, objectivity and transparency.

- Ensure that the investigation targets appropriate data sources (individuals as well as devices).
- Engage an objective third party with excellent credentials to manage the fact-finding process. It is not appropriate to ask employees to investigate their peers, and the involvement of a respected, disinterested party will help to reassure everyone.
- Immediately report findings to the appropriate agency. Obfuscation will only damage the organization’s credibility and increase the likelihood of additional scrutiny.

In the event of a federal investigation, be prepared to cooperate fully and efficiently.

- Develop a data map to track the devices from which you might need to collect data. Re-assess your environment regularly to keep the data map current.

1. Be prepared to perform forensic collections if required; as noted above, engage the assistance of certified forensic examiners. Even if your own IT staff is capable of properly performing a forensic collection, the objectivity that an outside expert will bring to the process, and the weight that proper certifications carry, will bring significant credibility to your efforts.

- Respond quickly and comprehensively, and provide requested data in the agency’s preferred format. If the agency does not request a specific format up front, determine their preferences and disclose any challenges you anticipate, offering your best available alternative production format(s).

Regardless of the nature of the investigation, use technologies and processes to effectively identify and assess potentially relevant materials.

- Partner with an experienced e-Discovery services provider to implement cost-effective technologies and methods:
 - » Use a reliable Early Data Assessment platform to search, cull and de-duplicate the collected data population.
 - » Use a document review application that offers sophisticated conceptual analytics. These technologies will help you quickly identify materials that contain key concepts, analyze trends in employees’ awareness of relevant issues, and assess potential culpability. Additionally, ensure that the platform supports an easy-to-manage workflow and highly granular auditing so that your review is thorough and defensible.
- If necessary, enlist the assistance of a reliable, on-shore review staffing firm to augment your in-house review teams by performing first-level reviews.

For more information about managing internal and federal investigations, visit <http://www.altep.com/discovery/data-forensics-investigations> or contact your local office: 602-264-3100

ⁱ Initial speech: Obama B. (June 17, 2009). Remarks by the President on 21st Century Financial Regulatory Reform. White House.

ⁱⁱ <http://apps.americanbar.org/buslaw/blt/2009-09-10/joshi.shtml>

Welcome New Members!

Alves, Charles

Arizona's G&T Cooperatives

Berry, Ryan

Spirit Realty Capital

Bishop, Anne

Delta Dental of Arizona

Borland de Marneffe, Katrin

Clear Channel Outdoor, Inc.

Burkett, David V.

Clear Channel Outdoor, Inc.

Davis, Isabel

Pragmatic Marketing, Inc.

Forkner, Matthew A.

Go Daddy Operating Company, LLC

Gillman, Brian S.

Mesa Air Group

Graham, Kathryn

Meracord, LLC

Greenberg, Benjamin M.

Discovery Land Company

Greenman, Ross E.

PAS Ltd.

Hall, Norman G.

Ashton Tiffany, LLC

Hennessee, J. Marc

IO

Holland, Jeffrey

Statesman Group of Companies

Kashak, Maya Y.

Sunquest Information Systems, Inc.

Levine, Scott

Universal Technical Institute, Inc.

LoCascio, Kelly K.

Aviation West Charters, Inc.

McAlpine, Cheree L.

Avnet, Inc.

Medina, Meggan E.

Cloudburst Consulting Group, Inc.

Nearhood, Richard D.

Ryan, LLC

Patel, Krishan

U-Haul International, Inc.

Pecora, Vincent

VIAD Corp

Schleuger, Gary

Universal Technical Institute Inc.

Shinohara, Gabrielle A.

Ventana Medical Systems, Inc.

Starita, Lisa M.

Element Payment Services, Inc.

Techera, Maria Eliset

Abeinsa EPC LLC

Toronyi Neuman, Kelli

Reachout Healthcare America

Wauro, Darlene M.

U-Haul International, Inc.

White, Jennifer E.

U-Haul International, Inc.

The Chapter wishes to
thank our 2013-2014
Newsletter Underwriter



Chapter Leadership

President**Mark Rogers**

Insight Enterprises, Inc.
Associate General Counsel & Assistant
Secretary
480.333.3475
mark.rogers@insight.com

Vice President**Robert Longo**

Waste Management, Inc.
Vice President & General Counsel,
Western Group
480.624.8417
rlongo@wm.com

Secretary**Gary Smith**

Phoenix Engine Services
General Counsel
602.284.7491
audric@cox.net

Treasurer**Kellen Brennan**

Universal Technical Institute, Inc.
Vice President & Assistant General
Counsel-Corporate Compliance
623.445.9348
kebrennan@uti.edu

Chapter Administrator**Karen Rogers**

accarizona@yahoo.com

Board of Directors**Mary Alexander****Margaret Gibbons****Sasha Glassman****David Glynn****Kevin Groman****Robert Itkin****Mary Beth Orson****Steven Twist****Cyndy Valdez**