# Governance Challenges:
# The Digital Side of Duty of Care

Josh Brower, Josh@DefensiveDepth.com

As a leader, there are many responsibilities to shoulder. One of the most difficult is that of protecting the assets under your care, whether they are physical, digital, or even personnel. With the continued integration of technology into every part of our lives, there is a legal requirement to protect our assets even in the digital world, specifically in the areas of personnel safety and customer information.

# 1. Introduction

It wasn't until the twentieth century and the second industrial revolution that common law evolved to include negligence outside of privity. With Donoghue v. Stevenson in 1932, the foundation of duty of care was laid. Also known as the Paisley Snail case, Mrs. Donoghue drank a bottle of ginger beer and fell sick because of a dead snail that had been accidentally bottled into it by the manufacturer, Mr. Stevenson. (Donoghue v Stevenson) Mrs. Donoghue sued the manufacturer, and eventually won, with Lord Atkin making the following statement

> ...You must take reasonable care to avoid acts or omissions which you can reasonably foresee would be likely to injure your neighbour. Who then in law is my neighbour? The answer seems to be—persons who are so closely and directly affected by my act that I ought reasonably to have them in contemplation as being so affected when I am directing my mind to the acts or omissions which are called in question... (Stone, 1965, p. 176)

With this foundational case in place, many subsequent cases resulted in refinement of this concept. In modern law, duty of care is mandated typically through statute or common law. When a claim is made that a duty of care has been breached, what is being stated is that the organization has failed to maintain their duty to care for their employees or clients and is negligent. (Claus, 2009) To successfully show negligence, the claim must incorporate the following:

"-the organization has a legal duty of care to conform to a certain standard,
-the organization fails to meet that standard, and
-the staff member is injured as a result of this failure." (Klamp, 2007, pp. 1-5)

While the conceptual framework of duty of care as outlined above remains mostly the same, the legal implementation varies widely internationally. This can create much confusion and concern for organizations that work internationally, and have employees traversing borders on a regular basis. If the employee wants to brings a suit against the organization, where will it be brought, and under which duty of care standards?

# 2. Current Realities of Digital Duty of Care

With the previous context in mind, let us look at the current realities of the digital aspect of duty of care. Though there are many aspects of duty of care that could be applied to the digital world, this paper will review two: including digital security as part of an organization's training program for employees, (especially when they are traveling or living abroad), and data breaches of an organization's customer's personal information.

When an organization has staff that travel or live outside of their home country, typically there is a briefing about where the employee is going, what would be some typical cultural faux pas to avoid, and the like. Depending on the organization and the destination, there will also be information or training for the staff in regards to personal safety, how to deal with bribes, and so

on. To do otherwise opens the organization up to all sorts of duty of care issues that could spring forth if a staff member is hurt or worse. With the advent of the World Wide Web, the explosion of social media, and the always-connected culture of the international business community, how does this affect personal safety awareness and training for staff that will be traveling? Consider the following examples:

A staff member is traveling to a region of the world that is currently embroiled in factional warfare, and there is a higher than average risk of kidnappings. The staff member wants to share about her trip with her online following, and posts to her social media accounts a photo of her (detailed) itinerary for the ten day trip.

A staff member of the PR department of a religious organization is traveling internationally for a month, and on the day of his departure, puts the following on his public social media accounts: *"Please pray for my family, as I will be traveling for a month, and they will be home alone."* His full name and home city is listed on his social media profiles, and his home address is easily obtained through public information sources.

An organization requires staff that travel internationally to use full disk encryption on their business laptops. They are told to never decrypt the drive for anyone without first consulting the organization's legal team. When a staff member goes through customs on an international trip, they refuse to decrypt the hard drive until they are able to make a phone call to their organization. Unfortunately, because of the time change, no one at the organization is available for at least six hours. The staff member undergoes an intense interrogation because they won't decrypt the hard drive during those six hours.

A staff member is traveling internationally and stops by an Internet cafe to catch up on business and personal correspondence. Unbeknownst to her, she has exposed herself to a high risk of identity theft because the Internet cafe computers were compromised with keyloggers and other malware.

All of the previous examples are based on true events. If the staff member's organization did not have sufficient training to help them understand the risks of social media when traveling, basic computing security, and how to deal with customs with encrypted devices, they have opened themselves up to a duty of care negligence case. I would submit to you that just as we perform personal (physical) safety awareness and training for staff, the training needs to take into account digital risks that the staff member might face when traveling. This training would help to reduce the risk of liability for this particular issue, as it shows that the organization not only foresaw potential harm, but also took reasonable steps to help prevent that harm from occurring. The type of training that should be used for this would need to be along the lines of SANS Securing the Human. (Securing the Human)

The second major area of digital duty of care is that of data breaches. According to PrivacyRights.org lists, since 2005 there have been over 867 million records compromised from 4,329 breaches that have been made public. (Chronology of Data Breaches) These breaches cover the gamut of the type of information compromised: payment card information, personal information, and medical information. There have been many high profile breaches in the last few years: Sony Corporation in 2011 (101 million records including usernames, passwords, name, address, country, email address, birth date) (Privacy Rights Clearinghouse), South Carolina Department of Revenue in 2012 (6.4 million personal tax records), (Privacy Rights Clearinghouse) Target (110 million records containing payment card information) in 2013, (Privacy Rights Clearinghouse) and Michaels (2.6 million records containing payment cards) in 2014, so far. (Privacy Rights Clearinghouse)

Though there is much outstanding litigation on the part of the customer against the aforementioned companies, there have not been many clear wins against the organizations. For instance, the major class action suit that was brought against Sony moved forward, but with the majority of the claims thrown out. (Balasubramani, 2014) In the spring of 2014 it was settled with Sony held liable for up to fifteen million dollars and almost three million dollars in attorney fees. (Orland, 2014) Even so, it remains clear that there must be a clearly delineated negligence in certain data breach incidents, as can be seen from the following excerpt from a recent article by John A. Fisher:

> At this point, the duty that should be required of businesses that deal with sensitive consumer data should be clear. Similar to the existing duty implicit in the FTC enforcement actions, businesses should have a legal duty to take reasonable care to protect sensitive consumer information from unauthorized access. As with the duty element of any negligence cause of action, one concern here is with the term "reasonable care." Since this Note seeks to ground the cause of action in a negligence per se theory, clarifying the term "reasonable care" as it applies to a company's security policies and implementation is straightforward. Anything that falls below the standards set by the kind of uniform federal legislation called for in Parts II and III will fail to constitute reasonable care. (Fisher, 2013)

In order to reduce the risk of liability for this particular issue, an organization must show that they not only foresaw potential harm, but also took reasonable steps to help prevent that harm from occurring. One reasonable step would be to start implementing the 20 Critical Security Controls for Effective Cyber Defense. (Critical Security Controls) These controls are an internationally recognized list of controls that if implemented correctly, will have a major positive impact on digital security in your organization.

## 3. Our Response

As can be seen, the current realities of the digital aspect of duty of care are extremely sobering. As leaders of our organizations, what should our response be? Should we care? I submit that we must take this issue seriously, as it is our moral duty, our legal duty, and it just makes business sense.

As leaders, we have a common moral obligation to protect not only the corporate assets under our leadership, but also the people that we lead and the customers that use our products and services. Consider what Lord Atkin stated in Donoghue v. Stevenson:

> The liability for negligence whether you style it such or treat it as in other systems as a species of "culpa," is no doubt based upon a general public sentiment of moral wrongdoing for which the offender must pay. But acts or omissions which any moral code would censure cannot in a practical world be treated so as to give a right to every person injured by them to demand relief. In this way rules of law arise which limit the range of complainants and the extent of their remedy. The rule that you are to love your neighbour becomes in law you must not injure your neighbour; and the lawyer's question "Who is my neighbour?" receives a restricted reply. You must take reasonable care to avoid acts or omissions which you can reasonably foresee would be likely to injure your neighbour. Who then in law is my neighbour? The answer seems to be persons who are so closely and directly affected by my act that I ought reasonably to have them in contemplation as being so affected when I am directing my mind to the acts or omissions which are called in question. (Kidner, 2012, p. 12)

It is an accepted moral obligation that we owe a duty of care to people from a physical perspective, why would this be any different when the landscape changes to the digital world?

From a legal perspective, it is clear that this issue is gaining more defined lines. We must keep ourselves aware of the changing legal landscape, and make sure that the way that we protect sensitive information and train our staff is in line not only with regulations, but also industry best practices, as duty of care typically goes beyond regulation, and takes into consideration what is the normative industry expectations in regards to the issue at hand.

Finally, from a business perspective, it just makes business sense to care and cater for these issues. The fallout from a breach or other digital incident has shown to be significantly more expensive and hurtful to the business than the financial cost of prevention and mitigation. The current actual cost to Target to deal with their 2013 breach exceeds sixty-one million dollars, though this does not take into account loss of sales from consumers taking their business elsewhere because of a lack of confidence. (McGrath, 2014) Looking at non-digital example, recall the record thirty-five million dollar fine assessed against GM by the USA Department of Transportation for their delay in reporting faulty ignition switches that have contributed to a

minimum of thirteen deaths. (Deluca, 2014) There are also a number of negligence lawsuits leveled at GM from the victims' families. What was the cost to mitigate the issue? Roughly one dollar per car. "It has to be money," said Beth Melton, mother of Brooke Melton, who died in a crash on her 29th birthday in 2010. "It has to come down to money but that really doesn't even make sense to me. **In the end, they're going to have to pay for it.**.." (Gutierrez, Gardella, Monahan, & Reynolds, 2014) (emphasis added)

## 4. Conclusion

In summary, this paper has given a brief introduction to duty of care, looked at a couple aspects of how duty of care applies to the digital world, and worked through what our response as leaders should be.

As we look to the future of duty of care and how it applies to the digital world, consider the following statement from John. A Fisher:

> ...More importantly, the notion that businesses only have a duty to guard against foreseeable risks of data breach places a burden on consumers to guard against breach as well...The burden on consumers to educate themselves and implement good Internet security practices is not meant as a device for allowing businesses to shrug off their duty of care. Quite the opposite, the burden on consumers should provide greater incentive to businesses to discover risks and notify consumers of them, so as to be able to make the argument that consumers should have been aware of the danger. (Fisher, 2013)

Though the above statement speaks specifically to data breaches, it would apply to the other issue that has been discussed—training organizational staff. In the future, we will see more of this mindset, that digital security is a shared responsibility between organization and staff and/or consumer.

As leaders, let us take these issues seriously and consider what needs to be adjusted in our organizations to be able to better protect and care for our most valuable assets - people.

*This paper provides only a discussion on general legal issues around duty of care, and does not constitute legal advice. International law is different for each potential case and every possible defendant. If you have a question regarding a specific situation, please obtain the legal advice of an attorney.*

# 5. References

(n.d.). Retrieved July 13, 2014, from Privacy Rights Clearinghouse: https://www.privacyrights.org/data-breach-asc?title=sony

(n.d.). Retrieved July 13, 2014, from Privacy Rights Clearinghouse: https://www.privacyrights.org/data-breach-asc?title=South+Carolina+Department+of+Revenue

(n.d.). Retrieved July 13, 2014, from Privacy Rights Clearinghouse: https://www.privacyrights.org/data-breach-asc?title=target

(n.d.). Retrieved July 13, 2014, from Privacy Rights Clearinghouse: https://www.privacyrights.org/data-breach-asc?title=Michaels

Balasubramani, V. (2014, January 29). *Sony PlayStation Data Breach Lawsuit Whittled Down but Moves Forward*. Retrieved July 13, 2014, from Technology & Marketing Law Blog: http://blog.ericgoldman.org/archives/2014/01/sony-playstation-data-breach-lawsuit-whittled-down-but-moves-forward.htm

*Chronology of Data Breaches*. (n.d.). Retrieved July 13, 2014, from Privacy Rights Clearinghouse: https://www.privacyrights.org/data-breach

Claus, L. (2009). *Duty of Care of Employers for Protecting International Assignees, their Dependents, and International Business Travelers.* International SOS.

*Critical Security Controls*. (n.d.). Retrieved July 23, 2014, from SANS.org: http://www.sans.org/critical-security-controls

Deluca, M. (2014, May 16). *GM to Pay Feds Record $35 Million Fine Over Deadly Ignition Fails*. Retrieved July 13, 2014, from NBC News: http://www.nbcnews.com/storyline/gm-recall/gm-pay-feds-record-35-million-fine-over-deadly-ignition-n107106

*Donoghue v Stevenson*. (n.d.). Retrieved July 13, 2014, from Scottish Council of Law Reporting: http://www.scottishlawreports.org.uk/resources/dvs/minitrial/

Fisher, J. A. (2013). Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach. *William & Mary Business Law Review*, 215-239.

Gutierrez, G., Gardella, R., Monahan, K., & Reynolds, T. (2014, March 13). *GM Chose Not to Implement a Fix for Ignition Problem*. Retrieved July 13, 2014, from NBC News: http://www.nbcnews.com/storyline/gm-recall/gm-chose-not-implement-fix-ignition-problem-n51731

Kidner, R. (2012). *Casebook on Torts.* Oxford University Press.

Klamp, C. (2007). Duty of Care. *Safety & Security Review*, pp. 1-5.

McGrath, M. (2014, February 26). *Target Profit Falls 46% On Credit Card Breach And The Hits Could Keep On Coming*. Retrieved July 13, 2014, from Forbes.com: http://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/

Orland, K. (2014, July 24). *Sony to pay up to $17.75 million in 2011 PSN hacking settlement*. Retrieved July 28, 2014, from Ars Techica: http://arstechnica.com/gaming/2014/07/sony-to-pay-up-to-17-75-million-in-2011-psn-hacking-settlement/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+arstechnica%2Findex+%28Ars+Technica+-+All+content%29&utm_content=Netvibes

*Securing the Human*. (n.d.). Retrieved July 23, 2014, from http://www.securingthehuman.org/: http://www.securingthehuman.org/

Joshua Brower, Josh@DefensiveDepth.com

Stone, J. (1965). *Human Law and Human Justice.* Stanford University Press.