From: Craig S Wright [craig@rcjbr.org]
Sent: 3/12/2008 6:39:15 PM
To: Dave Kleiman [dave@davekleiman.com]
Subject: FW: Defamation and the diffculties of law on the Internet.

I need your help editing a paper I am going to relase later this year. I have been working on a new form of electronic money. Bit cash, Bitcoin...

You are always there for me Dave. I want you to be a part of it all.

I cannot release it as me. GMX, vistomail and Tor. I need your help and I need a version of me to make this work that is better than me.

Craig

-----Original Message-----
From: dave kleiman [mailto:dave@davekleiman.com]
Sent: Wednesday, 12 March 2008 6:25 PM
To: security-basics@securityfocus.com
Subject: RE: Defamation and the diffculties of law on the Internet.

Hats off to you Craig,

Sometimes you amaze me....I literally today just took on a case today dealing exactly with this, you are making my life easy as I am gathering (with your permission) this information you have provided for my client's review.
When this becomes public record, I will post-up the results.

I will take any more information on this subject with great enthusiasm and appreciation, as always!!!

By the way, for those of you who have never asked for Craig's help, you do not know what you are missing.
I have asked his research assistance more than once. One particular time it was dealing with abilities of cookies on the server side, when I awoke the next morning, I had 100's of pages and links of information on that subject, and variations and ideas I had not even or forgotten to consider (e.g. web bugs). Why did he help, for no other than reason than he just likes to research information, and possibly considers me a friend from afar. He probably had as much fun reading up on the subject as did.
And along with all the technical details he included this:

Cookie Recipe Ingredients:
125 grams butter
50 grams caster sugar
60 grams brown sugar
1 large egg
1 teaspoon vanilla essence/extract
125 grams of plain flour
1/2 teaspoon salt
1/2 teaspoon bicarbonate of soda
250 grams of chocolate (Dark is best for this)
1/2 cup coarsely chopped almonds

Method: Turn your oven on to preheat at 180 degrees Celsius (about 350 degrees Fahrenheit, gas mark 4). Remember to take your grill pan out first. Now get some baking trays ready (if they're not non-stick then you better line them or grease them).....Hey Presto! The world's BEST cookies, in the comfort of your own home.

In the midst of this data exchange I casually mentioned that one day, when I was in the position to not have to work so much, I would return to school and my dream degrees in Cosmology and Astrophysics. Of course, the next day I had links to every online study available for those degrees, with a "Why wait wink."

Further, it amazes me how Craig has a Blog helping to understand the rights of US based Digital Forensic Examiners:

http://gse-compliance.blogspot.com/2008/01/texas-pi-fud.html
And he is based in AU. He simply cares enough about the cause and the industry to help, it has no direct affect on him if US DFEs are required to have PI licenses!!

People of the past considered "Loons":
(Feynman, Hawking, Sagan, da Vinci, Einstein, Columbus, everyone associated with Monty Python and the Holy Grail:
Black Knight: Right, I'll do you for that!
King Arthur: You'll what?
Black Knight: Come here!
King Arthur: What are you gonna do, bleed on me?
Black Knight: I'm invincible!
King Arthur: ...You're a loony.
.....you get the picture)

Yep Craig is a Junkie; a Knowledge Junkie!!!!

For those of you who have nothing good to say; why say anything?

Dave

Respectfully,

Dave Kleiman - http://www.davekleiman.com
4371 Northlake Blvd #314
Palm Beach Gardens, FL 33410
561.310.8801

> -----Original Message-----
> From: listbounce@securityfocus.com
> [mailto:listbounce@securityfocus.com] On Behalf Of Craig Wright
> Sent: Tuesday, March 11, 2008 17:15
> To: 'Simphiwe Mngadi'; security-basics@securityfocus.com
> Subject: RE: Defamation and the diffculties of law on the Internet.
>
> SANS had "Police Decline to Intervene in Libellous Bebo Page Case
> (March 7 & 8, 2008" in Newsbytes Vol 10.20.
>
> This refers to:
>
> http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article3498888.ece
> http://www.dailyrecord.co.uk/news/newsfeed/2008/03/07/web-of-lies-86908-20342677/
> http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2008/03/07/nbebo107.xml
>
> Actually, content control IS an aspect of security and compliance. I may have been a little angry when writing, but I am far from perfect.
>
> I have taken and updated a little something for the list based on responses I have received over the years. Liability against an Intermediary, whether in the traditional view of ISP and ICP as well as that of employers and other parties remains a risk.
>
> Extrusion filters seem to be something that is not considered, not by most organisations and not unfortunately by many of the list. There is more than filtering for attacks. This is surprising as many standards and regulations require that specific information is filtered. PCI-DSS, HIPAA and a raft of legislation specifies that organisation setup the capability to monitor both incoming and outgoing traffic. This is not port based, but rather a capability to monitor and filter (or at the least act on) content.
>
> I oversee the information gathering for many more companies than I actually audit myself (being an audit manager for an external audit firm). In 1,412 firms I have been to or reviewed information for, I

have collected a number of statistics over the years.
231 (or 16.4%) have some content management
184 (13.0%) have NO egress filters - Nothing at all. No ports Nothing.
734 (52.0% have a disclaimer on email that is barely adequate legally)
210 (14.8% have a legally valid privacy policy/disclaimer on their web sites)
15 (1.06% check Google or other places for information on their references)

In Scheff v Bock (Susan Scheff and Parents Universal Experts, Inc. v. Carey Bock - Florida USA, 2006, Case No. CACE03022837) a Florida jury awarded Sue Scheff US$11.3 million costs and damages over recurrent blog postings. A former acquaintance accused her of being a crook, a con artist and a fraudster (as a side note the same laws apply in Au).
See http://www.citmedialaw.org/threats/scheff-v-bock

In principle, defamation consists of a false and unprivileged statement of fact that is harmful to the reputation o f another person which is published "with fault". That is means that it is published as a result of negligence or malice. Different laws define defamation in specific ways that differ slightly, but the gist of the matter is the same. Libel is a written defamation; slander is a verbal defamation.

Some examples:
Libellous (when false):
Charging someone with being a communist (in 1959)
Calling an attorney a "crook"
Describing a woman as a call girl
Accusing a minister of unethical conduct
Accusing a father of violating the confidence of son

Not-libellous:
Calling a political foe a "thief" and "liar" in chance encounter (because hyperbole in context)
Calling a TV show participant a "local loser," "chicken butt" and "big skank"
Calling someone a "bitch" or a "son of a bitch"
Changing product code name from "Carl Sagan" to "Butt Head Astronomer"
See http://w2.eff.org/bloggers/lg/faq-defamation.php for details.

So let us do the Math. Let us take a case of 0.1% (or 1 in a thousand) employees (and the number is in reality higher then this) posting from their place of work a defamatory post. 83.6% of companies (based on figures above) will not detect or stop anything. Less check at all.

Let us take an average US litigation cost for defamation of $182,500 (taking cases won from 96 to current in Au, UK and US) Also see "Rethinking Defamation" by DAVID A. ANDERSON of the University of Texas at Austin - School of Law.
(http://papers.ssrn.com/sol3/papers.cfm?abstract_id=976116#PaperDownload).

So if we take a decent sized company of 5,000 employees, we have an expectation of 4 incidents per annum that in coming years would be expected to make it to court. Employers are vicariously liable for many of these actions. In the past, employers and ICP's have not been targeted, but this is changing. The person doing the act is generally not one with the funds to pay out the losses. The employer is. Thus the ability to co-join employers will increase these types of actions.

Facebook, blogs and other accesses will only make this worse in coming years.

So what does this mean? Well in the case of our hypothetical employer, there is an expected annualised loss of $788,400 US in coming years. The maximum expected payout would be $50,000,000 US. It is unlikely that the individual making the claim will be able to pay the cost of losing, so the employer will more and more be added to be suit.

Now, I am in no way affiliated with ANY content management software,

but I see this as a necessary evil. This would could as an effective corporate governance strategy, lowering the potential liability of the employer.

In my experience, the costs of the software and the management are going to add to less then the potential. With the recent win in Scheff v Bock, this is only going to increase.

Civil Liability
The conduct of both agents and employees can result in situations where liability is imposed vicariously on an organisation through both the common law[i] and by statute.[ii] The benchmark used to test for vicarious liability for an employee requires that the deed of the employee must have been committed during the course and capacity of their employment under the doctrine respondeat superior. Principals' liability will transpire when a `principal-agent' relationship exists. Dal Pont[iii] recognises three possible categories of agents:

(a) those that can create legal relations on behalf of a principal with a third party;
(b) those that can affect legal relations on behalf of a principal with a third party; and
(c) a person who has authority to act on behalf of a principal.

Despite the fact that a party is in an agency relationship, the principal is liable directly as principal as contrasting to vicariously, "this distinction has been treated as of little practical significance by the case law, being evident from judges' reference to principals as vicariously liable for their agents' acts"[iv]. The consequence being that an agency arrangement will leave the principle directly liable rather then liable vicariously.

The requirement for employees of "within the scope of employment" is a broad term without a definitive definition in the law, but whose principles have been set through case law and include:
where an employer authorises an act but it is performed using an inappropriate or unauthorised approach, the employer shall remain liable[v];

the fact that an employee is not permitted to execute an action is not applicable or a defence[vi]; and the mere reality that a deed is illegal does not exclude it from the scope of employment[vii].

Unauthorised access violations or computer fraud by an employee or agent would be deemed remote from the employee's scope of employment or the agent's duty. This alone does not respectively absolve the employer or agent from the effects of vicarious liability[viii]. Similarly, it remains unnecessary to respond to a claim against an employer through asserting that the wrong committed by the employee was for their own benefit. This matter was authoritatively settled in the Lloyd v Grace, Smith and Co.[ix], in which a solicitor was held liable for the fraud of his clerk, albeit the fraud was exclusively for the clerk's individual advantage. It was declared that "the loss occasioned by the fault of a third person in such circumstances ought to fall upon the one of the two parties who clothed that third person as agent with the authority by which he was enabled to commit the fraud"[x]. Lloyd v Grace, Smith and Co.[xi] was also referred to by Dixon J in the leading Australian High Court case, Deatons Pty Ltd v Flew[xii]. The case concerned an assault by the appellant's barmaid who hurled a beer glass at a patron. Dixon J stated that a servant's deliberate unlawful act may invite liability for their master in situations where "they are acts to which the ostensible performance of his master's work gives occasion or which are committed under cover of the authority the servant is held out as possessing or of the position in which he is placed as a representative of his master"[xiii].

Through this authority, it is generally accepted that if an employee commits fraud or misuses a computer system to conduct an illicit action that results in damage being caused to a third party, the employer may be supposed liable for their conduct. In the case of the principles agent, the principle is deemed to be directly liable.

In the context of the Internet, the scope in which a party may be liable is wide indeed. A staff member or even a consultant (as an agent) who publishes prohibited or proscribed material on websites and blogs, changes systems or even data and attacks the site of

another party and many other actions could leave an organisation liable. Stevenson Jordan Harrison v McDonnell Evans (1952)[xiv] provides an example of this type of action. This case hinged on whether the defendant (the employer) was able to be held liable under the principles of vicarious liability for the publication of assorted "trade secrets" by one of its employees which was an infringement of copyright. The employee did not work solely for the employer. Consequently, the question arose as to sufficiency of the "master-servant" affiliation between the parties for the conditions of be vicarious liability to be met. The issue in the conventional "control test" as to whether the employee was engaged under a "contract for services", against a "contract of service" was substituted in these circumstances with a test of whether the tort-feasor was executing functions that were an "integral part of the business" or "merely ancillary to the business". In the former circumstances, vicarious liability would extend to the employer. Similarly, a contract worker acting as web master for an organisation who loads trade protected material onto their own blog without authority is likely to leave the organisation they work for liable for their actions.

In Meridian Global Funds Management Asia Limited v Securities Commission[xv], a pair of employees of MGFMA acted without the knowledge of the company directors but within the extent of their authority and purchased shares with company funds. The issue lay on the qualification of whether the company knew, or should have known that it had purchased the shares. The Privy Council held that whether by virtue of the employees' tangible or professed authority as an agent performing within their authority[xvi] or alternatively as employees performing in the course of their employment[xvii], both the actions, oversight and knowledge of the employees may well be ascribed to the company. Consequently, this can introduce the possibility of liability as joint tort-feasors in the instance where directors have, on their own behalf, also accepted a level of responsibility[xviii] meaning that if a director or officer is explicitly authorised to issue particular classes of representations for their company, and deceptively issues a representation of that class to another resulting in a loss, the company will be liable even if the particular representation was done in an inappropriate manner to achieve what was in effect authorised.

The degree of authority is an issue of fact and relies appreciably on more than the fact of employment providing the occasion for the employee to accomplish the fraud. Panorama Developments (Guildford) Limited v Fidelis Furnishing Fabrics Limited[xix] involved a company secretary deceitfully hiring vehicles for personal use without the managing director's knowledge. As the company secretary will customarily authorise contracts for the company and would seem to have the perceptible authority to hire a vehicle, the company was held to be liable for the employee's actions.

Criminal Liability
Employers can be held to be either directly or vicariously liable for the criminal behaviour of their employees.

Direct liability for organisations or companies refers to the class of liability that occurs when it permits the employee's action. Lord Reid in Tesco Supermarkets Limited v Nattrass[xx] formulated that this transpires when someone is "not acting as a servant, representative, agent or delegate" of the company, but as "an embodiment of the company"[xxi]. When a company is involved in an action, this principle usually relates to the conduct of directors and company officers when those individuals are acting for or "as the company". Being that directors can assign their responsibilities, direct liability may encompass those employees who act under that delegated authority. The employer may be directly liable for the crime in cases where it may be demonstrated that a direct act or oversight of the company caused or accepted the employee's perpetration of the crime.

Where the prosecution of the crime involves substantiation of mens rea[xxii], the company cannot be found to be vicariously liable for the act of an employee. The company may still be found vicariously liable for an offence committed by an employee if the offence does not need mens rea[xxiii] for its prosecution, or where either express or implied vicarious liability is produced as a consequence of statute. Strict liability offences are such actions. In strict liability offences and those that are established through statute to

apply to companies, the conduct or mental state of an employee is ascribed to the company while it remains that the employee is performing within their authority.

The readiness on the part of courts to attribute criminal liability to a company for the actions of its employees seems to be escalating. This is demonstrated by the Privy Council decision of Meridian Global Funds Management Asia Ltd v Securities Commission[xxiv] mentioned above. This type of fraudulent activity is only expected to become simpler through the implementation of new technologies by companies. Further, the attribution of criminal liability to an organisation in this manner may broaden to include those actions of employees concerning the abuse of new technologies.

It is worth noting that both the Data Protection Act 1998[xxv] and the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000[xxvi] make it illegal to use equipment connected to a telecommunications network for the commission of an offence. The Protection of Children Act 1978[xxvii] and Criminal Justice Act 1988[xxviii] make it a criminal offence to distribute or possess scanned, digital or computer-generated facsimile photographs of a child under 16 that are indecent. Further, the Obscene Publications Act 1959[xxix] subjects all computer material making it a criminal offence to publish an article whose effect, taken as a whole, would tend to deprave and corrupt those likely to read, see or hear it. While these Acts do not of themselves create liability, they increase the penalties that a company can be exposed to if liable for the acts of an employee committing offences using the Internet.

[i] Broom v Morgan [1953] 1 QB 597.
[ii] Employees Liability Act 1991 (NSW).
[iii] G E Dal Pont, Law of Agency (Butterworths, 2001) [1.2].
[iv] Ibid [22.4].
[v] Singapore Broadcasting Association, SBA's Approach to the Internet, See Century Insurance Co Limited v Northern Ireland Road Transport Board [1942] 1 All ER 491; and Tiger Nominees Pty Limited v State Pollution Control Commission (1992) 25 NSWLR 715, at 721 per Gleeson CJ.
[vi] Tiger Nominees Pty Limited v State Pollution Control Commission (1992) 25 NSWLR 715.
[vii] Bugge v Brown (1919) 26 CLR 110, at 117 per Isaacs J.
[viii] unreported decision in Warne and Others v Genex Corporation Pty Ltd and Others -- BC9603040 -- 4 July 1996.
[ix] [1912] AC 716
[x] [1912] AC 716, Lord Shaw of Dunfermline at 739 [xi] [1912] AC 716 [xii] (1949) 79 CLR 370 at 381 [xiii] Ibid.
[xiv] [1952] 1 TLR 101 (CA).
[xv] [1995] 2 AC 500
[xvi] see Lloyd v Grace, Smith & Co. [1912] AC 716 [xvii] see Armagas Limited v Mundogas S.A. [1986] 1 AC 717 [xviii] Demott, Deborah A. (2003) "When is a Principal Charged with an Agent's Knowledge?" 13 Duke Journal of Comparative & International Law. 291
[xix] [1971] 2 QB 711 [xx] [1972] AC 153 [xxi] ibid, at 170 per Lord Reid [xxii] See Pearks, Gunston & Tee Limited v Ward [1902] 2 KB 1, at 11 per Channell J, and Mousell Bros Limited v London and North-Western Railway Company [1917] 2 KB 836, at 843 per Viscount Reading CJ.
[xxiii] See Mousell Bros Limited v London and North-Western Railway Company [1917] 2 KB 836, at 845 per Atkin J.
[xxiv] [1995] 2 AC 500.
[xxv] Data Protection Act 1998 [UK]
[xxvi] Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 [UK] [xxvii] Protection of Children Act 1978 [UK] [xxviii] Protection of Children Act 1978 and Criminal Justice Act 1988 [UK] [xxix] Obscene Publications Act 1959 [UK]

Regards,
Craig Wright (GSE-Compliance)

Craig Wright
Manager of Information Systems

Direct : +61 2 9286 5497
Craig.Wright@bdo.com.au
+61 417 683 914

BDO Kendalls (NSW)
Level 19, 2 Market Street Sydney NSW 2000
GPO BOX 2551 Sydney NSW 2001
Fax +61 2 9993 9497
http://www.bdo.com.au/