MAYER·BROWN

Text Messaging, Social Media Communication and the Risks They Present for Companies

February 19, 2014

1:00 -2:00 p.m. EST

Social Media Webinar

William Michael Jr.
wmichael@mayerbrown.com

Catherine A. Bernard
cbernard@mayerbrown.com

Speakers

William Michael Jr.
Chicago
+1 312 701 7653
wmichael@mayerbrown.com

Catherine A. Bernard
Washington D.C.
+1 202 263 3405
cbernard@mayerbrown.com

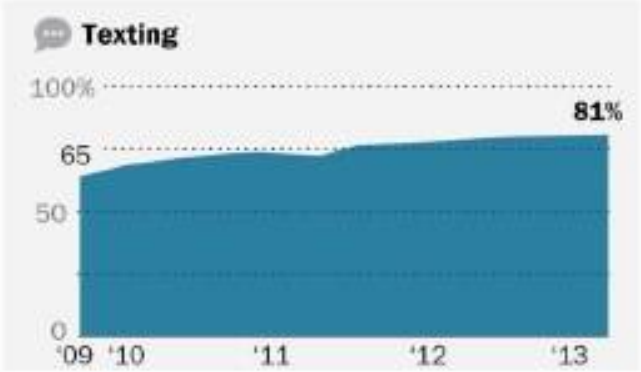
Agenda

- Statistics and Notable Cases
- E-Discovery Considerations
  - Discoverability
  - Retention/Duty to Preserve/Spoliation
  - Admissibility
- Corporate Policy Considerations
- Levels of Access to Individual's Information and the Applicable Legal Framework
  - Corporate vs. Individual Devices
  - Password Protected Information
  - False Accounts
  - Publicly Available Information

STATISTICS AND NOTABLE CASES

Statistics: Text Messaging

- 91% of adults in the United States own mobile phones
  - 81% send and receive text messages
  - Nearly a third (31%) prefer texting to calling
- Gen Y are by far the most avid users of text messages
  - 97% of U.S. adults between 18 and 24 own mobile phone
  - This population sends or receives an average of 109.5 messages per day



Source: Pew Research, "Cell Phone Activities 2013" (http://www.pewinternet.org/2013/09/19/cell-phone-activities-2013/)

What Does This Mean for Employers?

- Young adults entering the workforce bring their communications preferences along with them
- Content is unpredictable: the conventions and features of e-mail do not apply
  - Proper use of subject lines
  - Appropriate signatures
  - Automatic spell-check before sending
  - Metadata stripping
- Casual real-time feel + widespread assumption that deletion of texts is irreversible can lead to sticky situations…

Notable Cases: BP/Deepwater Horizon

- BP engineer Kurt Mix deleted more than 500 text messages relating to the April 2010 explosion of the Deepwater Horizon oil rig
  - Because Mix used a smartphone, federal investigators were able to recover all but 17 of the messages
  - Contained estimates of oil spill rates up to 3x higher than public disclosures
  - Forensic methods showed that Mix had deleted the messages 16 months after receiving a legal hold notice for all records, including texts
- Serious consequences:
  - BP pled guilty to criminal charges and paid $4.5 billion in penalties; largest criminal fine in history
  - Mix was convicted of obstructing justice in December 2013; faces up to 20 years in jail and $250k in fines

Notable Cases: Fort Lee Traffic Disaster

- Closure of lanes on the NJ side of the George Washington Bridge turned into a still-simmering scandal for NJ Gov. Christie after emails/texts were released:

(Fort Lee Mayor)

Sent 9/10/13 8:04 AM

Sokolich text to Baroni: Presently we have four very busy traffic lanes merging into only one toll booth..... The bigger problem is getting kids to school. Help please. It's maddening

Received 9/10/13 8:05 AM

Is it wrong that I am smiling?

Sent 9/10/13 8:05 AM

No

Received 9/10/13 8:05 AM

I feel badly about the kids

Received 9/10/13 8:06 AM

I guess

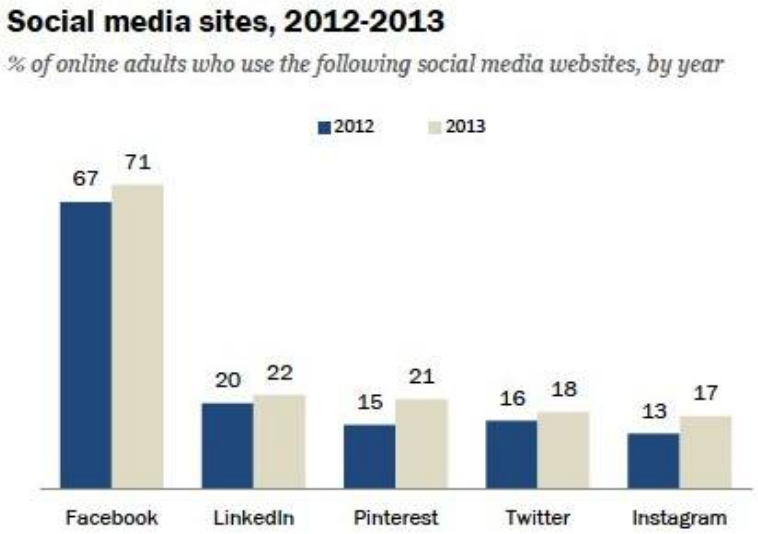
Sent 9/10/13 8:11 AM

They are the children of Buono voters

Top Christie Aide

Statistics: Social Media

- 73% of online adults use at least one social networking site
  - Facebook remains king (71% of online adults), but use of other sites is increasing, chiefly LinkedIn, Pinterest, Twitter, and Instagram
  - Most Facebook and Instagram users visit those sites at least once a day



- 90% of Gen Y uses at least one social media platform (esp. Facebook); other groups not far behind

Sources: Pew Research, "Social Networking Fact Sheet" (http:// www.pewinternet.org/fact-sheets/social-networking-fact-sheet/); "Social Media Update 2013" (http://www.pewinternet.org/2013/12/30/social-media-update-2013/)

What Does this Mean for Employers?

- Digital trails can't be separated into business v. leisure
  - Employee use is essentially impossible to prevent
  - Social media communications travel fast and far
  - Once it's out, you can't get it back

Notable Cases: NetFlix CEO Reed Hastings

- On July 3, 2012, Hastings posted on the Netflix Facebook page:

- Stock price jumped 13%
- Resulted in a "Wells notice" – warning that SEC may bring an enforcement action against Netflix for violating Reg FD
  - Reg FD requires companies to disclose material non-public information to all investors at the same time
  - Did Netflix violate Reg FD by disclosing this information only to subscribers to the company's Facebook page?
- SEC opted not to sue Netflix; companies now can disclose news through social media "so long as investors have been alerted about which social media will be used to disseminate such information"

Notable Cases: Former NY Mayoral Candidate Anthony Wiener

E-DISCOVERY CONSIDERATIONS

Uncharted Territory in E-Discovery

- Our digital trails are growing larger and ever more varied
  - Status updates/posts
  - Instant messages
  - Tweets (and retweets)
  - Blogs
  - Photo and video sharing
  - "Follows"
  - "Likes"
  - "Pokes"
  - Comments
  - Groups/causes joined
  - Activity streams
  - Apps downloaded
  - Location "check-ins"

All may qualify as discoverable electronically stored information (ESI) under FRCP 34:

"writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form"

Uncharted Territory in E-Discovery

- Regulators and plaintiffs' firms are waking up to the opportunities created by text/social media evidence
- Digital trail left by plaintiffs presents opportunities for defendants as well, particularly in class and consumer actions, where discovery obligations typically are imbalanced
  - *EEOC v. Original Honeybaked Ham* (D. Colo. 2012)
    - EEOC alleged that Defendant had subjected a class of female employees to sexual harassment and retaliation
    - Defendant sought the contents of class members' email, text messages, and social media accounts
    - Court agreed that this content was discoverable; privacy concerns over information created for sharing were minimal and could be accomodated by use of a special master and *in camera* review
- Widespread use of abbreviations, lingo, and misspellings may make use of search keywords and/or predictive coding difficult

Discoverability Challenges

- Stored Communications Act: *Mintz v. Mark Bartelstein & Assocs.* (C.D. Cal. 2012)
  - Plaintiff, a sports agent, sued to have a non-compete clause declared unenforceable; former employer countered with trade secret claims
  - Court agreed that Stored Communications Act precluded AT&T from disclosing the content of plaintiff's text messages
  - But because terms of service contract gave plaintiff the right to obtain copies of his messages on demand, he had "control" for purposes of FRCP 26 and could be required to produce in response to a simple document request
- Relevance : *Robinson v. Jones Lang LaSalle Americas, Inc.* (D. Or. 2012)
  - Plaintiff sued for employment discrimination, claiming emotional distress
  - Court ordered production of all of plaintiff's social media communications in any way relevant to "any significant emotion, feeling, or mental state allegedly caused by defendant's conduct" over a 4-year period

Discoverability Challenges

- Relevance – another view: *Giachetto v. Patchogue-Medford Union Free Sch. Dist.* (E.D.N.Y. 2012)
  - Teacher diagnosed with ADHD sued school district under the ADA and NY State Human Rights Law for discrimination and failure to make adequate accommodations
  - Defendant moved to compel plaintiff to authorize release of all records from her social networking accounts
  - Court denied motion as to routine status updates/communications, but agreed that any postings referencing (1) events alleged in the complaint or (2) plaintiff's claimed emotional distress (including other potential sources of distress) were relevant
  - Plaintiff's counsel was ordered to conduct an independent review of all records for relevance; could not rely on client's assessment

Retention Considerations

- Critical to establish a routine retention policy (which may, and sometimes should, include a policy that such information is not preserved at all)
- Text messages present data retrieval issues – becomes a balance of importance v. difficulty
  - Different devices have different storage and backup mechanisms
  - Readability and length
  - Expense – may require extensive forensic work
- Consider whether company Facebook pages, Twitter feeds, etc. should be archived locally
  - May save time and money in complying with discovery requests
  - But keep in mind that the stronger the policy, the more data there is to mine
- Regulated industries may have particularized retention requirements

Collection Challenges

- Text and social media ESI present unique complications
  - Several steps may be needed to produce a record in a useable, understandable format
  - To minimize time and cost, think ahead:
    - Do you have a collection tool that can be integrated with your e-discovery software?
    - Do you have a method for aggregating content (e.g., a Facebook page) into a usable, understandable format?
    - Do you have a plan for imaging devices (especially if your policy is BYOD)?
    - Is a process in place to document collection decisions and the reasoning behind them?
  - Where will you draw the line about what is "reasonably accessible?"

Duty to Preserve/Spoliation

- Duty to preserve and safeguard all potentially relevant ESI is triggered when litigation filed, threatened, or reasonably foreseeable
- Courts have not hesitated to impose hefty sanctions or adverse inferences
- *In re Praxada Product Liability Litigation* (S.D. Ill. 2013)
  - Defendants were sanctioned $931,500 for failing to suspend auto-deletion of text messages between sales force and supervisors
- *Regas Christou v. Beatport, LLC* (D. Colo. 2013)
  - Defendant issued a legal hold instructing employees to preserve text messages, but did not take steps to collect the data; key defendant lost his iPhone
  - Court allowed an adverse inference instruction
- *U.S. v. Suarez* (D.N.J. 2010)
  - Government failed to instruct agents not to delete text messages with a cooperating witness; late litigation hold meant that many of the texts were not preserved on servers/backup tapes
  - Court allowed an adverse inference instruction

A New Twist –Self-Destructing Communications

- The wildly popular Snapchat app allows users to share photos that automatically delete after a few seconds of viewing
  - According to Snapchat, the images disappear from its servers as well
  - Screenshot capability creates a giant loophole
  - Message's digital trail is logged (to/from, date, time)
- New Confide app is marketed as Snapchat for business communications
  - Messages appear in blocked-out format; must swipe to reveal
  - Once read, messages are destroyed immediately
  - Alerts sender if a screenshot is taken
  - Unclear what kind of digital trail is logged

Admissibility of Text/Social Media Communications

- The susceptibility of texts/social media to manipulation and falsification creates hurdles to admissibility
- Authentication issues should be considered from the start
  - Courts have held that internet printouts are authenticated by witness declaration and circumstantial indicia of authenticity. *Kennerty v. Carrsow-Franklin (In re Carrsow-Franklin)*, 456 B.R. 753, 756–57 (Bankr. D.S.C. 2011).
  - Other methods to consider: data establishing that a particular computer or device was used to create or post the information; requests for admission
  - Again, documentation of collection/preservation efforts is key
- Evidentiary case law allows messages to be admissible even absent proof that the message was received, opened or read. Those points go to the weight of the evidence, not admissibility.

Admissibility: What About Hearsay?

- As a general rule, hearsay rules apply to texts and social media just as they do to other evidence
- But little guidance from the courts on how existing hearsay doctrine can be made to accommodate the nature of text and social media evidence:
  - Is a search on WebMD admissible as a "statement made for medical diagnosis or treatment?"
  - Is a text in ALL CAPS an "excited utterance?"
  - Is a status update admissible as a "recorded recollection?"
  - Is a retweet or "like" an "adoptive admission?"
  - Are postings on a company's official Facebook page "business records?"
  - Is a comment on a genealogy website a "statement of personal or family history?"

CORPORATE POLICIES

Corporate Policies – Key Considerations

1. How Texting and Social Media Do – or Do Not – Fit Into the Organization's Business
2. Integration of Policies and Procedures Into Existing Compliance and Supervisory Programs
3. Definition of Social Media
4. Level of Access Employees Have to Social Media on Work Devices During Work Hours
5. Employee Use of Social Media on Personal Devices on Personal Time
6. Level of Company Access to Employee's Work vs. Personal Devices
7. Level of Company Access to Information Stored on Social Media sites

ACCESS: PERSONAL DEVICES

Bring Your Own Device (BYOD)

- One of the biggest risks presented by employees' bringing their own devices is company data loss.
- Companies can mitigate risks by implementing policies outlining appropriate behavior, usages, and security software for BYOD devices.
- Accessing social media on these privately owned devices presents additional hurdles for the employer: employees have an increased expectation of privacy when using a personally owned device.

Case Study: Text Messages

- If on a work device, employer likely has broad access rights, even to personal messages, especially if illegal or improper activity is suspected
  - See, e.g., *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010)
  - A California police officer claimed supervisors' search of his text messages violated his Fourth Amendment rights. The officer was using a city-issued pager to send explicit messages.
  - Court found that the City's search was proper, but failed to establish any bright line rules, stating that courts should not use the case to "establish far-reaching premises that define the existence, and extent, of privacy expectations" of workers.

Case Study: Text Messages

- If on a personal device, employers rights will be more limited from a practical and privacy perspective.
  - Internal Investigations vs. Litigation: may need a court order to even obtain the device or data
  - Quon and its progeny indicate that on the balance, the employees right to privacy will be greater

ACCESS: USERNAMES & PASSWORDS

Employer Requesting Password Access

- Employers have tried to access employee social media by requesting employees to reveal usernames and passwords.
- Varying degrees of coercion: simply ask, stating that participating is voluntary, demand it as a term of hiring or continued employment.
- Restricted by many states, though state-by-state limitations vary.

Employer Requesting Password Access

- Currently, legislation has been enacted or proposed in more than 35 states.
- 12states have enacted laws restricting employer access to employee passwords: Arkansas, California, Colorado, Illinois, Maryland, Michigan, Nevada, New Jersey, New Mexico, Oregon, Utah and Washington.
- Other states are still developing legislation: New Hampshire, Oklahoma.
- National enforcement challenging, similar to data breach laws

Employer Requesting Password Access

- Case law also indicates that wholesale access to password-protected information is not allowed by an employer, especially where a policy does not provide as such.
- Pure Power Boot Camp v. Warrior Fitness Boot Camp (S.D.N.Y. 2010)
    - The employer's email policy informed employees that the employer could access "any matter stored in, created on, received from, or sent through" the employer's system.
    - The employer obtained the usernames and passwords for the employee's web-based, personal email accounts (i.e., hotmail/gmail) on the employee's work computer and used this information to access the employee's web-based email accounts and read his email.
    - The court found that, where the employee did not actually send or receive the email from the work computer, but merely viewed the email from a work computer, the employer's broad-ranging email policy was not sufficient to prevent the employee from having a reasonable expectation of privacy in the content of his web-based email accounts: "there is nothing in the PPBC policy that even suggests that if an employee simply views a single, personal e-mail from a third party e-mail provider, over PPBC computers, then all of his personal e-mails on whatever personal e-mail accounts he uses, would be subject to inspection."

Employer Requesting Password Access

Pure Power Boot Camp v. Warrior Fitness Boot Camp (S.D.N.Y) (continued)

- Accordingly, the court said that the employee had a reasonable expectation that "his personal e-mail accounts, stored on third-party computer systems, protected (albeit ineffectively) by passwords, would be private" and that the employer's access would be authorized only if the employee had given consent.
- Because the employee had a reasonable expectation of privacy, the employers viewing of the email constituted unauthorized access under the Stored Communication Act, and the employer was prohibited from using the emails as evidence in the underlying labor and employment action between the parties.
- This case, though it pertains to email, is especially applicable to social networks, because all of the communications on social networks is stored on remote servers. An employee may never actually post anything to the social networking site from work, but the employee's username and password might be stored on her work computer.

Employer Requesting Password Access

- See also Electronic Communications Privacy Act (ECP) 18 U.S.C. § 2511
- Whoever "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" commits a violation.
- *Hall v. EarthLink Network, Inc.*
  - EarthLink, an internet service provider, did not violate the ECPA because of a particular exception that was applicable to it as an Internet Service Provider that stored email from the employee as part of its "ordinary course of business."
  - But the Court specifically noted that if a company sets up any mechanism to continually receive and view email transmissions from an employee, the employer likely violates the ECPA, because this is an interception of electronic communications.
  - Thus, if an employer set up a system allowing it to continually monitor email transmissions as they were sent, or social media posts as they were posted, a Court could determine it violated the ECPA.

Shoulder Surfing

- Shoulder surfing refers to the practice of employers asking employees to log onto social media accounts while the employer looks on.
- This happens in the context of hiring , firing, and internal investigations.
- There have been many recent attempts to prevent employers from doing this. In 2012, states including Maryland, California, and Illinois banned this practice.

Keystroke Software

- Keystroke software can be installed on the computer itself, or it can operate remotely through a "Trojan horse" email. In either situation, the information is sent back to the employer for review.
- The software can track application use, log-ons, screen shots, passwords, document tracking, and many other computer activities.
- Keystroke software is directly regulated by some states, and can also fall under some of the other statutes discussed throughout this presentation.

ACCESS:
FALSE ACCOUNTS

False Accounts: CFAA

- Computer Fraud and Abuse Act (CFAA) 18 U.S.C. § 1030(a)
- Prohibits accessing a computer without authorization.
- An employer who accesses a social networking site surreptitiously – e.g., by assuming a false identity to "friend" an employee on Facebook – may violate the terms of service of the social networking site. An employer may violate the terms of service merely by conducting a background investigation on the site, if the site's terms of service prevent such activity.
- By violating the terms of service of the website, the employer could be deemed to have accessed the "computer" housing the social media website without authorization – technically a violation of the Computer Fraud and Abuse Act (CFAA).

False Accounts: CFAA

- CFAA allows the government to prosecute a criminal violation – unlikely given the breadth of the statute and the low stakes involved for the USAOs.
- However, private plaintiffs can also bring a claim under CFAA, and the language of the statute would seem to allow employees – not just the owners of the computer at issue – to bring a claim: "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).
- Thus, by accessing Facebook's website without authorization (i.e., in violation of the terms of service) an employee who claims he/she was harmed as a result could technically bring a claim for a violation of CFAA as a result.

False Accounts: CFAA

- United States v. Drew
  - Defendant set up a fake profile on the social networking site MySpace – a practice which violated the site's Terms of Service.
  - The defendant used the fake profile to harass a 13-year-old girl, who committed suicide after the harassment. At trial, the defendant was found guilty of a criminal misdemeanor violation of CFAA, and the defendant then moved for judgment of acquittal.
  - The court held that basing a misdemeanor violation of CFAA solely upon the violation of a website's terms of services is unconstitutional under the void-for-vagueness doctrine. However, the decision leaves open the possibility that a defendant may still face civil penalties under CFAA for violating a website's terms of service.

False Accounts: SCA

Stored Communications Act (SCA) 18 U.S.C. § 2701

- Designed to address access to stored wire and electronic communications and transactional records. "Whoever— (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility."
- The SCA "protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility." *Theofel v. Farey-Jones,* 341 F.3d 978, 982 (9th Cir. 2003). It "reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility." *Id.* at 982.

False Accounts: SCA

Pietrylo v. Hillstone Restaurant Group (D.N.J.)

- Employees set up an invite only website on MySpace.com that criticized their employer.
- The employer asked one of the employees for her username and password to the website, and she provided it.
- Based on what the employer saw on the website, it terminated some employees
- Employees sued under the Federal Stored Communications Act, and brought common law claims for invasion of privacy, and wrongful termination among other claims.
- The Court denied the employer's summary judgment motion and set the case for trial, ruling that a jury had to determine whether the employer's mere request for the username and password was coercive, and therefore the employer did not have actual authorization to access the website.

False Accounts: SCA

Pietrylo v. Hillstone Restaurant Group (D.N.J.) (continued)

- A jury ruled that the employer was not properly authorized to access the website under the Stored Communication Act because its request to the employee for her username and password was coercive. This ruling was based solely on the employee's own testimony that she felt that there may have been negative consequences if she did not give her employer her password.
- The Court upheld the jury's verdict in 2009. The employer was held liable for lost wages to the plaintiffs and punitive damages in the amount of four times the lost wages.

False Accounts: SCA

- In 2013, a New Jersey District Court held in *Ehling v. Monmouth-Ocean Hospital* that the SCA applies to Facebook posts.
- Because "the legislative history of the [SCA] suggests that Congress wanted to protect electronic communications that are configured to be private," the court determined that Plaintiff's private Facebook wall post fell under the SCA's protections.
- However, the employer here was not found liable because the post was volunteered by a "friend" of the Plaintiff who had access to the Plaintiff's Facebook posts.

False Accounts: Ethical Opinions

- Additionally, courts have indicated that employers should not create false social media accounts to circumvent the laws discussed above. Such action may be a violation of the terms of the social media user agreement.
  - *Fteja v. Facebook, Inc.* (S.D.N.Y. 2012) (holding that employers can be civilly liable for violating social media's user agreements)
- Lawyers especially should not be involved in the creation of such accounts—found to be
  - New York Formal Op. 2010-2 (cannot use false pretenses to obtain evidence)
  - Philadelphia Opinion 2009-02 (ethical rules violated where a third party, at request of a lawyer, sends a connection request)

ACCESS: PUBLIC INFORMTION

Publicly Available Information

- Publicly available information comes with fewer pitfalls for companies, but care should still be taken when viewing and relying on that information
- Can be used as evidence of discrimination
  - *Neiman v. Grange Mutual Casualty Co*.(C.D. Ill. April 26, 2012) (finding evidence that the company used information available on LinkedIn to discriminate against a potential employee based on age)
- Could have confidential information
  - *See, e.g.,* Title II of the Genetic Information Nondiscrimination Act of 2008 (GINA), 42 U.S.C. § 2000ff-1(a). GINA prohibits employers from obtaining an applicant's "genetic information," defined to include information about an individual's family medical history.
- Should know details of specific social media site
  - For example, LinkedIn has a feature where can see who has viewed a profile—could raise ethical issues for lawyers, especially if other person is represented.

Summary

- Publicly available information is generally fair game ***with*** parameters
- False accounts to gain information are not advisable and can lead to sanctions
- In certain circumstances can get information through passwords and usernames, but weigh the balance of importance against difficulty, and check state statutes
- Law is adapting in this area slowly to ever changing technology and trending towards the protection of employees' privacy
- While damages have not yet been significant for violations the risk is that damages will increase

MAYER·BROWN

Thank you for joining us.

Questions? Please email evilleda@mayerbrown.com