Socially Aware: The Social Media Law Update

2011 Best Law Firm Newsletter

THE BURTON AWARDS FOR THE PURSUIT OF PERFECTION

IN THIS ISSUE

Welcome to the June 2012 issue of *Socially Aware*, our Burton Award-winning guide to the law and business of social media! In this issue, we take a look at legislative efforts to prohibit employers from demanding disclosure of Facebook passwords from employees and job applicants; summarize guidance from California regulators regarding social media use by financial institutions; discuss a recent case holding that Facebook "likes" do not constitute protected speech under the First Amendment; examine a controversial New York court decision finding that a defendant had no proprietary or privacy interests in his tweets; explore a new decision limiting the scope of the Communication Decency Act's safe harbor for interactive computer service providers from defamation and other claims; highlight key "takeaways" for businesses from the FTC's recent privacy report; and provide a brief overview of Twitter's online legal documents. All this plus some interesting statistics on the impact of user-generated content on Generation Y's purchasing decisions, and Status Updates, our round-up of social media news items.

To stay on top of social media law developments between issues of our newsletter, please follow us on our blog, www.sociallyawareblog.com, and on Twitter, @MoFoSocMedia.

EDITORS

John Delaney
Gabriel Meister
Aaron Rubin

CONTRIBUTORS

Jessica Childress
Nicholas Datlowe
Reed Freeman
Susy Hassan
Erin Herlihy
Heidi Johanns
Matthew R. King
Alexander Lawrence
Leo Martin
Julie O'Neill
Debbie Rosenbaum
Cecilia Ziniti

Lawmakers Rush to Ban Employers From Demanding Facebook Passwords

In response to press reports that employers are increasingly demanding that employees and job applicants disclose their login information for Facebook and other social media sites, state and federal legislatures have jumped into action, with Maryland recently becoming the first state to expressly prohibit the practice.

A number of states are poised to follow Maryland. Currently, California, Illinois, Massachusetts, Michigan, Minnesota, New Jersey, and Washington have bills in the pipeline that seek to ban employers from requesting confidential login information as a condition of employment, and these bills appear to be attracting broad, bipartisan support.

The new Maryland law, which will go into effect on October 1, 2012, prohibits employers from requesting employees' social media passwords. The law applies to "employers" – broadly defined as any person engaged in a business, industry, profession, trade or other enterprise in Maryland, as well as units of Maryland state and local government – and their respective representatives and designees, and even employers that are based outside Maryland but that have employees located in Maryland will need to comply with the statute.

When it takes effect, Maryland's new law will prohibit covered employers from:

- Requesting or requiring an employee or applicant to disclose his or her user name, password, or any other means of accessing a personal account or service through computers, telephones, PDAs, and similar devices;
- Taking disciplinary action against employees for their refusal to disclose certain password and related information; and
- Threatening to take disciplinary action against employees for their refusal to disclose such information.

However, employers are not entirely prohibited from accessing employees' personal accounts. Under certain circumstances, Maryland's new law will allow employers to access employees' personal accounts in order to investigate the following (in each case, only if the employer has received information regarding such conduct):

- Whether an employee is complying with securities or financial laws or regulatory requirements, if the employee is using a personal website, Internet website, web-based account or similar account for business purposes; or
- An employee's actions regarding his or her downloading of the employer's proprietary information or financial data to a personal website, Internet website or web-based account.

The bill that led to the Maryland law gained widespread support after a state resident, Robert Collins, made headlines when he was asked to disclose his Facebook password to be recertified as a correctional officer with the Maryland Department of Public Safety and Correctional Services. Reportedly, the department had a practice of reviewing applicants' social media profiles to ensure that they were not engaged in any illegal activities and, believing he had no other option, Collins disclosed his Facebook username and password to his interviewer for the correctional officer position.

Federal law may also soon prohibit employers from requesting employees' social media passwords.

California appears to be getting closer to adopting its own law prohibiting this practice. Two relevant bills are currently pending in California, one of which (AB 1844) the California Assembly passed on May 10, 2012, and one of which (SB 1349) was passed by the California Senate on May 25, 2012. Both bills seek to prohibit employers from requiring employees and prospective employees to disclose user names or account passwords to access personal social media accounts. SB 1349 goes one step further, preventing employers from even requesting such user names and account passwords unless in connection with an investigation of "harassment, discrimination, intimidation or potential violence," and only then if the employee is not required to provide the requested information. SB 1349 also specifically prohibits employers from taking adverse action against employees "in any way for refusing to disclose the requested information related to their personal social media account."

Federal law may also soon prohibit employers from requesting employees' social media passwords. Despite an initial hiccup when the U.S. House of Representatives rejected Democratic Congressman Ed Perlmutter's proposed amendment to the Federal Communications Commission Reform Act, which would have prohibited this practice, additional efforts have been made to achieve substantially the same result through alternative means.

On April 27, 2012, Congressman Eliot Engel (D-NY) proposed H.R. 5050, the Social Networking Online Protection Act, or "SNOPA," in the United States House of Representatives. If passed, this bill would impose a nationwide ban on the practice of employers requiring or requesting access to their employees' online personal accounts. Similar to the new Maryland law, H.R. 5050 broadly defines employers who are covered under the law – for purposes of the law, "employer" includes "any person acting directly or indirectly in the interest of an employer in relation to an employee or an applicant for employment." The House bill, which prohibits institutions of higher learning and local educational agencies

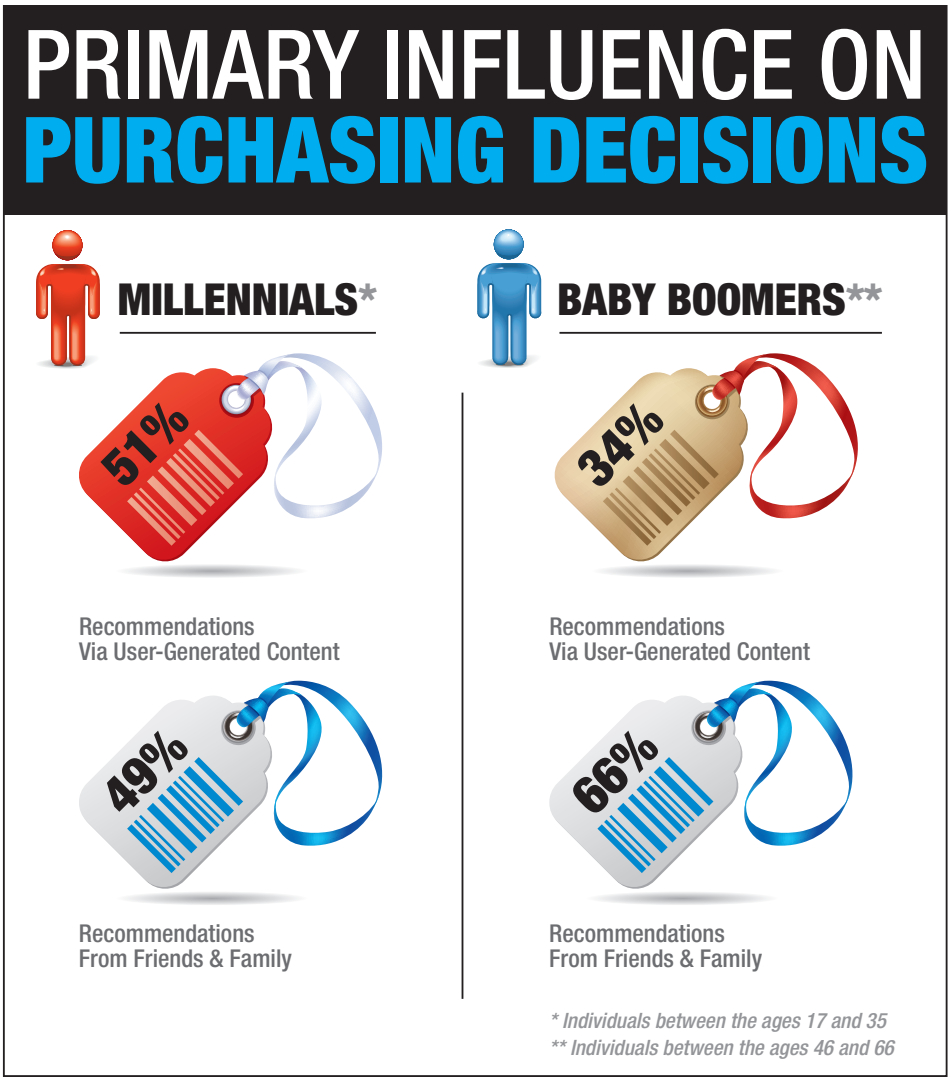
Employers can minimize their exposure to claims of discriminatory hiring practices by refraining from viewing applicants' online profiles during the application process.

from requesting the passwords of students or prospective students, is even broader in scope than the new Maryland law.

Shortly after H.R. 5050 was introduced, on May 9, 2012, Senators Richard Blumenthal (D-CT), Chuck Schumer (D-NY), Ron Wyden (D-OR), Jeanne Shaheen (D-NH), and Amy Klobuchar (D-MN) introduced the Password Protection Act of 2012 (S.B. S. 3074) ("PPA") in the Senate, and Congressmen Heinrich (D-NM) and Perlmutter (D-CO) introduced a parallel bill in the House. The PPA would amend the Computer Fraud and Abuse Act and prohibit employers from requiring or requesting access to employees' online personal accounts or password-protected computers, provided that such computers are not the employer's computers. The PPA would also prohibit employers from taking adverse actions against employees for refusing to disclose such passwords and, under the PPA, employees would be eligible to receive compensatory damages and injunctive relief if their employers were found to have violated the Act.

These efforts illustrate clearly the growing opposition to requiring current or potential employees to disclose their personal account passwords. Similar incidents of employers requesting access to their current and prospective employees' accounts have surfaced around the United States, with some employers taking disciplinary action for employees' refusal to disclose password information. As a result, Facebook, as well as privacy advocates, have publicly opposed the growing practice of employers requesting access to employees' social media profiles. U.S. Senators Richard Blumenthal and Charles Schumer have also sent letters both to the U.S. Department of Justice, asking it to investigate whether this practice violates the Stored Communication Act or the Computer Fraud and Abuse Act, and to the U.S. Equal Employment Opportunity Commission, asking that agency to opine whether the practice violates existing anti-discrimination laws.

It is clear that, even in the absence of statutory authority prohibiting employers from requesting access to current and future employees' social media profiles, employers should exercise caution when seeking access to employees' or prospective employees' social media accounts. For example, although a job applicant's social media profile may be publicly available, when viewing the applicant's profile, a potential employer may learn information that would otherwise remain undisclosed in the application process, such as an applicant's membership in a protected class (we noted this issue with respect to current employees' social media profiles back in November 2011). Employers can minimize their exposure to claims of discriminatory hiring practices by refraining from viewing applicants' online profiles during the application process. For this and other



Source: Talking to Strangers: Millennials Trust People Over Brands, Jan. 2012

reasons, employers – whether in Maryland or elsewhere – are urged to carefully consider potential legal risks when instituting policies related to accessing their current and prospective employees' online personal accounts.

California Provides Social Media Guidance for Financial Institutions

While Facebook, Twitter, LinkedIn and other social media platforms have become increasingly important tools for businesses across industries to meet their customers' needs and expectations, financial institutions have been slow to embrace social media. This is likely attributable to the highly regulated environment in which financial institutions operate, the unique risks associated with operating within it, and the lack of available guidance on how to navigate and mitigate such risks.

In an effort to address industry concerns, the California Department of Financial Institutions ("DFI") – the licensing and regulatory agency that oversees California's state-chartered financial institutions – recently conducted a survey of more than 340 financial institutions' use of social media policies. The survey revealed that 72 percent of the financial institutions surveyed did not have a social media plan, and 59 percent did not have a social media policy. These findings suggest that either a significant number of financial institutions are not utilizing social media or they are doing so without the important framework needed to help ensure that they do not run afoul of their many regulatory requirements.

To that end, the DFI has published guidance on the development of social media policies. The guidance first addresses how a financial institution should go about developing a social media plan, specifically, by asking itself a variety of questions that form the basis for plan development, including:

- What does your financial institution expect to gain from using social media?
- Who are the target viewers?
- What types of bank activities and postings are planned?
- What types of social media do you plan to use and how do you plan to use them?
- How will the activities be managed and by whom?

The DFI's guidance also identifies the elements necessary for a financial institution's creation of appropriate social media policies. These include:

- A description of approved social media activities;
- Guidelines for personal use, if allowed;
- Definition of permitted content;
- Inclusion of applicable consumer protection laws and regulations requirements, if the institution's products and services will be advertised;
- Employee training; and
- Identification of oversight responsibility.

The DFI's three-part series was published in the December, February and March issues of its *Monthly Bulletin*. The DFI plans to continue to cover these issues in subsequent bulletins.

The DFI is not the only regulatory body that is taking action in this area. The Federal Financial Institutions Examination Council ("FFIEC") – the interagency body tasked with prescribing uniform principles, standards and report forms for the federal examination of financial institutions – has charged a task force with developing guidance on financial institutions' use of social media. In addition, the Financial Industry Regulatory Association ("FINRA") – an independent regulator of securities firms – has published basic guidance in the form of two Regulatory Notices, one in January 2010 and the other in August 2011.

The survey revealed that 72 percent of the financial institutions surveyed did not have a social media plan, and 59 percent did not have a social media policy.

While greater input may be required from financial industry regulators as corporate use of social media continues to evolve, the DFI frameworks and the guidance provided by FINRA are the pragmatic first steps needed by an industry that seems to have partly steered clear of this potentially large, growing, and indispensable channel for reaching its consumers. Financial institutions should seriously consider reviewing these materials when creating their own plans and policies.

What's Not to "Like"? Facebook Usage and the First Amendment

In the recent decision in *Bland v. Roberts*, the federal District Court for the Eastern District of Virginia held that merely "liking" a Facebook page is insufficient speech to merit constitutional protection.

Five former employees of the Hampton Sheriff's Office brought a lawsuit against Sheriff B.J. Roberts, in his individual and official capacities, alleging that he violated their First Amendment rights to freedom of speech and freedom of association when he fired them — allegedly for having supported an opposing candidate, Jim Adams, in the local election against Roberts for Sheriff. In particular, two of the plaintiffs had "liked" Jim Adams's page on Facebook. When Sheriff Roberts was reelected, he terminated the plaintiffs as

employees, but did not cite the Facebook likes or other support of Jim Adams as reasons for their departures.

The two plaintiffs alleged that they engaged in constitutionally protected speech when they liked the Jim Adams Facebook page. In April 2012, however, the court granted Roberts's motion for summary judgment, ruling that a Facebook "like" does not meet the standard for constitutionally protected speech. (The freedom of association claims were dismissed under the theories of qualified and Eleventh Amendment Immunity.)

The court looked to other cases involving speech on social media websites, noting that precedent had developed around cases where the speech at issue involved actual statements (e.g., *Mattingly v. Milligan* and *Gresham v. City of Atlanta*). The court held that this case was distinguishable because liking involved no actual words, and constitutionally protected speech could not be inferred from "one click of a button." In summary, the court wrote that liking a Facebook page is "not the kind of substantive statement that had previously warranted constitutional protection."

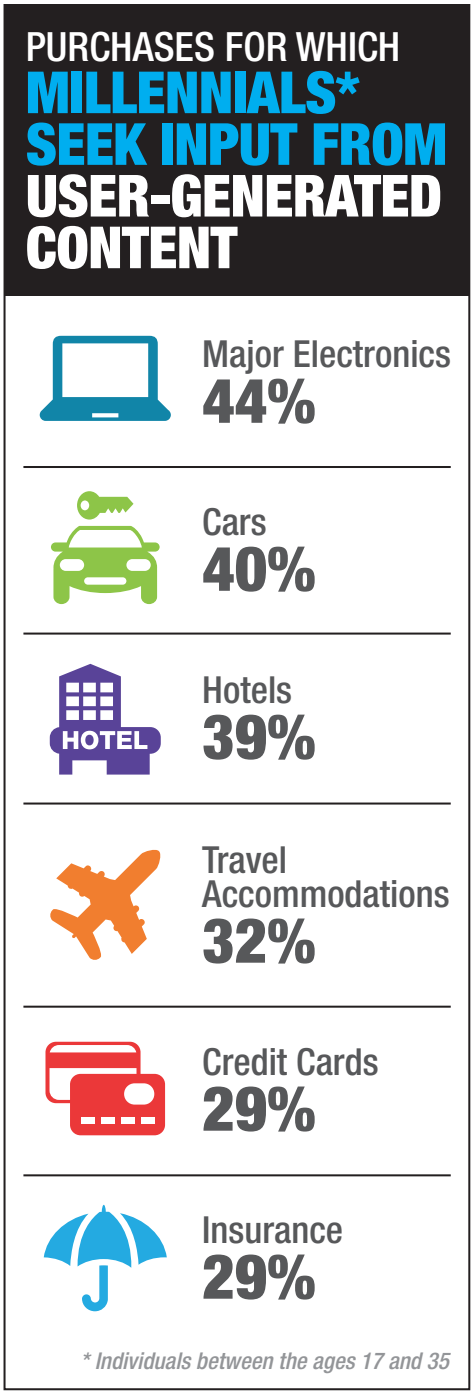
Because it ruled that liking a Facebook page cannot be considered constitutionally protected speech, the court did not proceed to analyze whether the plaintiffs' First Amendment rights had been violated. The court based its decision on the fact that the plaintiffs made no actual statements, suggesting that had there been a declarative statement—such as a wall post—the court's decision might have been different. (One of the plaintiffs alleged that he had written a wall post with an expressed opinion, but deleted the post before it could be documented.) Critics point out that the court's ruling that protected speech requires an actual statement is inconsistent with prior First Amendment case law, which identifies various forms of protected speech (e.g., armbands in *Tinker v. Des Moines Independent Community School District*; flag burning in *Texas v. Johnson*). This point is a key issue ripe for appeal.

Internet law experts argue that the court failed to consider the technology behind liking a page on Facebook. For example, Professor Eric Goldman, a prominent legal scholar and blogger, has observed that liking is more than a passive signal of virtual approval and that the like functionality has various effects on Facebook's algorithm, including increased publicity for the liked page. Although it is unclear whether these underlying changes are sufficient to tip the protected speech scale, Goldman and others argue that these changes should at least be weighed in the court's decision.

The question for the social media community moving forward is whether other courts will agree that liking should not amount to constitutionally protected speech. Regardless of the outcome, the case provides a good lesson: like it or not, what you say on a social media network can be used against you.

New York Court to Criminal Defendant: Your Tweets Can and Will Be Used Against You

In past issues of *Socially Aware*, we have discussed using subpoenas in civil litigation to obtain evidence from social media sites, including whether individuals have a privacy interest in this information and how the Stored Communications Act may limit the use of subpoenas in civil cases. Until now, we have not discussed these issues in the context of a criminal case. Does the prosecutor have to get a search warrant to obtain information about someone's social media use? Does the Stored Communications Act limit the government's authority in this area? A decision from the Criminal Court of the City of New York arising out the Occupy Wall Street movement, *People of the State of New York v. Malcolm Harris*, sheds some light on these questions.



Source: Talking to Strangers: Millennials Trust People Over Brands, Jan. 2012

On October 1, 2011, protesters marched on the Brooklyn Bridge as part of an Occupy Wall Street demonstration. Malcolm Harris, along with hundreds of other protesters, was charged with disorderly conduct for allegedly occupying

the roadway of the Brooklyn Bridge. The District Attorney expected Harris to claim as a defense that he stepped onto the roadway because the police led him there. The District Attorney, however, asserted that Harris, while on the bridge, may have tweeted statements inconsistent with his anticipated defense.

The District Attorney issued a third-party subpoena on Twitter, seeking user information and tweets associated with the account @destructuremal, allegedly used by Harris. Harris notified Twitter that he would move to quash the subpoena, and Twitter took the position that it would not comply with the subpoena absent a ruling by the court. The District Attorney opposed the motion.

The court found that Harris lacked standing to quash the third-party subpoena on Twitter. The court found that Harris had neither a proprietary interest nor a privacy interest in the user information and tweets associated with the account. The court denied Harris's motion to quash, and ordered Twitter to comply with the subpoena.

No Proprietary Interest in Tweets

First, according to the court, Harris's tweets were not his tweets. When registering a Twitter account, the user must agree to Twitter's Terms of Service, which includes a grant to Twitter of a "worldwide, non-exclusive, royalty-free license to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute" user content posted to Twitter. The court found that Twitter's license to use Harris's tweets meant that the tweets posted by Harris "were not his." In the court's view, Harris's "inability to preclude Twitter's use of his [t]weets demonstrates a lack of proprietary interest in his [t]weets."

No Privacy Interest in Tweets

The court went on to reject Harris's contention that he had a privacy interest in his tweets. Twitter's Terms of Service also state that submitted content "will be able to be viewed by other users of the Service and through third party services and websites," and Twitter's Privacy Policy states that the Twitter's service is "primarily designed to help you share information with the world." Twitter makes no assurances of privacy. Rather, Twitter notifies its users that their tweets (at least on default settings) will be available for the world to see. Thus, the court found that tweets are "by definition public."

No Search Warrant Required

The court further held that Harris's Fourth Amendment rights were not at issue, because the Internet is not a physical "home." While service providers may refer to a user's space on the site as a "virtual home," the court took the position that this "home" is no more that "a block of ones and zeros stored somewhere on someone's computer." Thus, while Twitter users may think that the Fourth Amendment protections that apply in their physical homes will also apply to their Twitter accounts, "in reality, the user is sending information to the third party, Twitter."

No Stored Communications Act Protection

Finally, the court held that, unlike in a civil case, the Stored Communications Act permits the government in a criminal case to subpoena subscriber and session information directly from the social media site. The court held that, unlike private litigants in civil litigation, prosecutors may obtain such information using any federal or state grand jury, trial or administrative subpoena by showing "specific and articulable facts showing that there are reasonable grounds to believe" that the tweets "are relevant and material to an ongoing criminal investigation." The court held that the District Attorney clearly made this showing in the case.

In short, the court has made it clear that users of social media who also find themselves charged with a criminal offense should have no expectation that potentially relevant information will be considered private or beyond the reach of a subpoena.

Reaction to Decision

The court's decision has been criticized by tech blogs and the American Civil Liberties Union, and, on May 7, 2012, Twitter filed a motion to quash the court's order, arguing that among other errors in the court's decision, under Twitter's Terms of Service, Harris in fact retained his rights to any content that he submitted, posted or displayed on or through the Twitter service. We'll keep in eye on further developments in this case.

A Dirty Job: TheDirty.com Cases Show the Limits of CDA Section 230 Immunity

We've reported before on Section 230 of the Communications Decency Act (CDA), the 1996 statute that states, "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Courts have interpreted Section 230 to immunize social media and other websites from liability for publishing content created by their users, provided the site owners are not "responsible in whole or in part, for the creation or development of" the offending content.

Two recent federal cases involving the website TheDirty.com show that, 15 years after the landmark *Zeran v. AOL* case interpreting Section 230 immunity broadly, courts still grapple with the statute and, arguably, get cases wrong, particularly when faced with unsavory content.

TheDirty.com is an ad-supported website that features gossip, salacious content,

news and sports stories. The site, run by owner/editor Hooman Karamian, a/k/a Nik Richie, prompts users to "submit dirt" via a basic text form requesting "what's happening" and "who, what, when, where, why," and allows users to upload files. In response, users, referred to on the site as the "Dirty Army," submit stories and photographs along with gossip about the people pictured. Richie then posts the pictures and information, often accompanied by his own comments. Two such racy posts, one detailing the sex habits of a Cincinnati Bengals cheerleader and the other about the supposed exploits of a "Church Girl," led their subjects to bring defamation claims in federal court. Third-party users, not TheDirty.com, generated the content. Cases dismissed on Section 230 grounds, right? Not quite.

In *Jones v. Dirty World Entertainment Recordings*, a case in the U.S. District Court for the Eastern District of Kentucky, plaintiff Sarah Jones, a cheerleader for the Cincinnati Bengals football team and also a high school teacher, sued TheDirty.com based on two user-submitted posts that included her picture and statements regarding her sex partners, as well as allegations that she had sexually transmitted diseases. Richie added a one-line comment— "why are all high school teachers freaks in the sack?"—and published the post. Jones requested that the posts be removed, but TheDirty.com refused. Richie also commented on the site directly addressing Jones, saying that her concern about the post was misguided and that she was "d[igging] her own grave" by calling attention to it. Jones sought damages for defamation and invasion of privacy under state tort law, and TheDirty.com moved for judgment as a matter of law on CDA immunity grounds.

The court held that TheDirty.com did not qualify for CDA immunity because it "specifically encouraged the development of what is offensive about the content" (citing the Tenth Circuit's opinion in *Federal Trade Comm'n v. Accusearch*). The court found that the TheDirty.com encouraged the development of, and therefore was responsible for, the offensive content based on the site's name, the fact that the site encouraged the posting of "dirt," Richie's personal comments added to users' posts, and his direct reference to the plaintiff's request that the post be taken down. The court focused on Richie's comments, including his statement, "I love how the Dirty Army has war mentality. Why go after one ugly cheerleader when you can go after all the brown baggers."

To hold that a website operator loses immunity based on the mere potential that users will post defamatory content effectively vitiates CDA immunity and parts ways with cases like the Ninth Circuit's *Roommates.com* case.

The *Jones* court's analysis diverges from prevailing CDA case law in a few respects. For example, regarding the issue of responding to a subject's request that an allegedly defamatory post be taken down, the Ninth Circuit has held that deciding what to post and what to remove are "traditional duties of a publisher" for which the CDA provides immunity to website operators. More critically, in adopting the "specifically encouraged the development of what is offensive" standard coined in *Accusearch*, the court in *Jones* reasoned that by requesting "dirt," the site "encourage[d] material which is *potentially* defamatory or an invasion of the subject's privacy," and therefore lost CDA immunity. That reasoning, though, could extend to any website functionality, such as free-form text boxes, that permits users to input potentially defamatory material. To hold that a website operator loses immunity based on the mere potential that users will post defamatory content effectively vitiates CDA immunity and parts ways with cases like the Ninth Circuit's *Roommates.com* case, which held that a website's provision of "neutral tools" cannot constitute development of content for purposes of the exception to CDA immunity. For these and other reasons, one leading Internet law commentator calls the case a "terrible ruling that needs to be fixed on appeal." TheDirty.com's appeal to the Sixth Circuit is pending.

In a more recent case, *S.C. v. Dirty World, LLC*, the U.S. District Court for Western District of Missouri held that Richie and TheDirty.com *did* qualify for CDA Section 230 immunity on facts similar to those in *Jones*. The plaintiff in *S.C.* brought suit based on a user-generated post on TheDirty.com that showed the plaintiff's picture along with a description alleging that she had relations with the user's boyfriend and attempted to do so with the user's son. Richie published the post, adding a comment about the plaintiff's appearance. The court explained that, because a third party authored the allegedly defamatory content, CDA immunity turned on whether TheDirty "developed" the content by having "materially contribute[d] to [its] alleged illegality." The court held that the defendants did not materially contribute to the post's alleged illegality because the defendants never instructed or requested the third party to submit the post at issue, "did nothing to specifically induce it," and did not add to or substantively alter the post before publishing it on the site.

After having noted these facts, and how they differed from the facts in *Jones*, which the *S.C.* plaintiff had cited, the court explicitly "distanced itself from certain legal implications set forth in *Jones*." The *S.C.* court pointed out that a "broad" interpretation of CDA immunity is the accepted view. It explained that CDA immunity does not, and should not, turn on the "name of the site in and of itself," but instead focuses on the content that is actually defamatory or otherwise gives rise to legal liability. The court noted, for example, that the site itself has a variety of content, much of it not defamatory or

capable of being defamatory (*e.g.*, sports stories and other news).

Given that some may consider TheDirty.com's gossip content and mission extreme, cases like *S.C.* are likely to provide peace of mind to operators of more conventional social media sites. Still, should *Jones* survive appeal, it could lead to forum shopping in cases where plaintiffs expect to face CDA immunity defenses, because the "specifically encouraged" standard could, as in *Jones*, lead to a loss of immunity. We'll keep you posted on the appeal.

FTC's Privacy Report Suggests Tightening of Privacy Regime, Provides Guidance to Business

On March 26, 2012, the Federal Trade Commission (the "Commission" or "FTC") released its much-anticipated final privacy report, *Protecting Consumer Privacy in an Era of Rapid Change*. The report builds upon the Commission's December 2010 preliminary report, and provides recommendations for businesses and policymakers with respect to online and offline privacy practices. The report will be of interest to any company using social media for marketing purposes. Specifically, the report:

- **Presents a privacy framework that sets forth best practices – not legal requirements – for businesses.** The Commission states that, to the extent that the best practices set forth in the report extend beyond existing legal requirements, such best practices are not intended to serve as a template for law enforcement actions or regulation under laws currently enforced by the Commission. FTC Chairman Jon Leibowitz reiterated this point to a House Energy and Commerce subcommittee on March 29, 2012, informing legislators that, while companies that follow the report's best practices would not be in violation of the FTC Act, those that do not follow them would not necessarily be in breach of the law. In his words, the report "is not a regulatory document or an enforcement document." That said, those elements of the report that focus on transparency and consumer choice build on the Commission's recent law enforcement experience; it is therefore reasonable to assume that the Commission will continue its pattern of focusing on data practices that are not obvious to consumers in context, that are not disclosed adequately, and, in some instances, where consumers do not have meaningful choice. Of course, the Commission will continue its aggressive enforcement of companies' privacy and data security promises.

- **Recommends baseline privacy legislation.** In the Commission's view, because self-regulation has not yet gone far enough, flexible and technologically neutral baseline privacy legislation is desirable. While encouraging industry to continue its self-regulatory efforts, the Commission also intends the privacy framework set forth in the report to assist Congress in crafting legislation. The Commission also reiterates its call for federal information security and data breach notification legislation and for legislation regulating the practices of data brokers.

- **Highlights the Commission's privacy priorities for the coming year.** The report explains that the Commission will promote implementation of the privacy framework by focusing its efforts on five main areas:
(1) cooperation with industry to complete the implementation of an easy-to-use, persistent and effective ***Do Not Track*** mechanism (the Commission does *not* call for Do Not Track legislation in this report);

The FTC will continue its pattern of focusing on data practices that are not obvious to consumers in context, that are not disclosed adequately, and, in some instances, where consumers do not have meaningful choice.

(2) improvement of privacy disclosures and other protections offered by ***mobile services***, including through its May 30, 2012 public workshop on revisions to its Dot Com Disclosures guidance; (3) support for targeted legislation to give consumers access to the information about them held by ***data brokers*** and encouragement to data brokers that compile data for marketing purposes to create a centralized website to further increase the transparency of their practices; (4) exploration of the privacy issues associated with the comprehensive tracking of consumers' online activities by ***large platform providers***, such as ISPs, operating systems, browsers and social media in a workshop later this year; and (5) participation with the Department of Commerce and industry stakeholders to create ***enforceable self-regulatory codes of conduct***.

This final priority reflects the Commission's support for the report issued by the Obama administration on February 23, 2012. In its report, entitled *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, the administration detailed a "Consumer Privacy Bill of Rights" and announced the

creation of a multi-stakeholder process to be convened by the Department of Commerce to create voluntary codes of conduct which, if adopted by companies, would be enforceable by the Commission pursuant to its deception authority under Section 5 of the FTC Act. Importantly, the Commission's report makes clear that the FTC will participate in the Department of Commerce's multi-stakeholder process.

The Scope of the Privacy Framework

The privacy framework applies to all commercial entities that collect or use online and/or offline consumer data that can be reasonably linked to a specific consumer or computer or other device. There is an exception for entities that collect only non-sensitive data from fewer than 5,000 consumers per year and do not share the data with third parties, so as not to unduly burden small businesses. The Commission did not, however, exempt from the framework's intended coverage those companies already covered by sector-specific privacy laws, such as the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act. Instead, the Commission emphasizes in the final report that the framework is intended to foster best practices but not impose conflicting legal obligations, and urges Congress not to pass legislation that creates overlapping or contradictory requirements for entities subject to such laws.

The extension of privacy best practices to data linkable to a computer or other device reflects the Commission's position that the line between "personally identifiable information" ("PII") and "non-PII" is increasingly blurred. The Commission justified this application on the grounds that, not only is re-identification of supposedly "anonymous" data increasingly possible, but, in the Commission's view, businesses have strong incentives to re-identify such data.

To provide businesses with certainty with respect to what constitutes "reasonably linkable" data, the Commission has taken the position that data are not "reasonably linkable" – and therefore not within the scope of the privacy framework — if the company possessing such data implements the following protections: (1) reasonable measures to ensure that the data are de-identified; (2) a public commitment to using the data in a de-identified way; and (3) contractual prohibitions on downstream entities that use the data from de-identifying the data, coupled with reasonable measures to ensure compliance with that prohibition. Even with this attempt at clarity, questions remain, including what it means to "de-identify" data. For example, does this mean removing PII or does it mean removing any identifier, such as cookie IDs? Furthermore, what measures are "reasonable" in terms of monitoring downstream entities?

The Substance of the Privacy Framework

The Commission's report proposes a privacy framework that calls for companies to incorporate "**privacy by design**" into their practices, to offer consumers ***simplified choices*** about how their data are collected and used, and to provide consumers with ***greater transparency*** about their practices.

Privacy by Design

According to the report, companies should promote consumer privacy throughout their organizations and at every stage of the development and life cycle of their products and services. As a substantive matter, this means that companies should incorporate the following privacy protections into their practices:

- **Reasonable security for consumer data.** The Commission notes that this obligation is already well settled, as it has a long history of enforcing data security obligations under Section 5 of the FTC Act and other laws. The Commission commends industry's efforts to ensure the security of consumers' data, but, nonetheless, it renews its call for Congress to enact comprehensive data security and breach notification legislation.
- **Reasonable limits on data collection.** According to the Commission, reasonable limits are those that are consistent with the context of a particular transaction or the consumer's relationship with the business (or as required or specifically permitted by law).
- **Sound retention and disposal practices.** The Commission states that companies should implement reasonable restrictions on the retention of consumer data and should dispose of such data once the data have outlived the legitimate purpose for which they were collected. What is "reasonable" depends on the type of relationship and the nature and use of the data.
- **Data accuracy.** According to the Commission, companies should maintain the accuracy of the data they hold about consumers. As with other elements of the framework, the Commission believes that the best approach to achieving accuracy is through a flexible approach, scaled to the intended use and sensitivity of the data at issue.

The Commission also urges businesses to maintain comprehensive data management procedures throughout the life cycle of their products and services. The Commission cites its recent settlement orders with Facebook and Google as providing a roadmap for the types of comprehensive procedural protections it envisions: (1) designation of personnel responsible for the privacy program; (2) a risk assessment that covers, at a minimum, employee training, management and product design and development; (3) implementation of controls designed to mitigate identified risks; (4) appropriate oversight; and (5) evaluation and adjustment of the program in light of regular testing and monitoring.

As a general matter, data use and disclosure practices that are inconsistent with the context of the transaction or the company's relationship with the consumer require consumer choice.

Simplified Consumer Choice

The report encourages companies to simplify consumer choice, in part by identifying those practices for which choice is not necessary. Specifically, the report provides that companies do not need to provide consumers with choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer or that are required or specifically authorized by law. While this standard relies to some degree on consumer expectations, it focuses on objective factors related to the consumer's relationship with the business. The following commonly accepted practices are provided as examples of the kinds of practices that do not typically require consumer choice: product and service fulfillment, internal operations, fraud prevention, legal compliance and public purpose and first-party marketing.

The report goes on to address practices that require choice and states that, when choice is required, it should be offered at a time and in a context in which the consumer is making a decision about his or her data. (The Commission declines, however, to impose any particular method of providing choice, leaving it to industry to develop the most appropriate choice mechanisms.) As a general matter, ***data use and disclosure practices that are inconsistent with the context of the transaction or the company's relationship with the consumer require consumer choice*** (unless such practices are required or specifically authorized by law). Such practices may include, for example, sharing customer data with an affiliate for the affiliate's own direct marketing use, if the consumer would not have been aware of the affiliate relationship (e.g., because the companies are differently branded).

The Commission identifies two practices that it believes require ***affirmative express consent:*** (1) in connection with ***material retroactive changes to privacy representations*** (this is not new, as the Commission has expressed it repeatedly for years and has imposed it in settlement orders); and (2) ***before collecting sensitive data***, such as information about children, health and financial information, geolocation data and Social Security numbers. (The Commission also proposes that social networks and others specifically targeting teens should take extra precautions with respect to their submission of personal information.) The Commission's identification of specific practices that require affirmative express consent suggests that, where it otherwise calls for choice, clear and conspicuous notice and opt-out would be sufficient.

Greater Transparency

The Commission states that companies should increase the transparency of their data practices, through privacy notices, access to data and consumer education:

- Privacy notices should be ***clearer***, ***shorter and more standardized***, to enable better comprehension and comparison of privacy practices. The Commission calls for the simplification of privacy notices, such as through the use of standardized terminology, format and other elements. In the Commission's view, members of various industry sectors should work together to create standards relevant to their industry, possibly through the multi-stakeholder process that the Department of Commerce plans to convene. According to the Commission, the need for simplification and industry involvement is particularly acute in the mobile realm, given the number of entities that want to collect user data and the limited space for disclosures. As noted above, the Commission plans to address mobile disclosures in a May 30, 2012 public workshop.
- Companies should provide ***reasonable access*** to the consumer data they maintain. The extent of access should be proportionate to the sensitivity of the data and the nature of its use. For example, the Commission urges businesses that maintain data for marketing purposes to, at a minimum, provide consumers with access to such data and permit them to suppress categories they would not like used for targeting.
- Companies should make efforts to ***increase the transparency of their data enhancement practices***. The Commission does not suggest that companies obtain consent to such practices; however, it urges industry to rely on the other elements of the privacy framework to address the privacy concerns raised by it. In the Commission's view, this means that companies should, for example, explain to consumers how data enhancement works and how they can contact data enhancement sources directly. Companies should also encourage their data sources to increase their own transparency.
- The Commission encourages companies to continue to engage in ***consumer education*** efforts and invites industry to re-brand and use the Commission's own materials.

Conclusion

The report reflects the Commission's continued concern that consumers bear too much of a burden for understanding and controlling how their data are collected, used, retained and disclosed. The report reflects its desire to see this

paradigm reversed so that the burden is shouldered by companies instead. How far this concern is turned into enforceable requirements will depend in large part on the support the Commission receives from Congress, as well as the extent of the development and adoption of self-regulatory codes of conduct.

Twitter's Twists, Turns and Terms: A Brief Overview of Twitter's Online Legal Documents

In our September 2010 issue of *Socially Aware*, we provided a brief overview of Facebook's "Statement of Rights and Responsibilities," the social media service's complex set of terms and conditions that companies frequently "click-accept" with little or no review (often in a rush to establish their Facebook presences). Naturally, this situation is not limited to Facebook; for many if not most social media services, when users first sign up for an account, they are required to agree to the service's lengthy standard terms and conditions of use. It's part of life on the Internet.

Twitter is no exception. When you sign up for a Twitter account — *"By clicking the button, you agree to the terms below"* — Twitter's core Terms of Service, that is, which are shorter than Facebook's Statement of Rights and Responsibilities but similarly link and branch off to a variety of policies, guidelines and related documents, all of which govern your use of Twitter's "various websites, SMS, APIs, email notifications, applications, buttons, and widgets."

At the top of Twitter's hierarchy of terms and conditions are the Twitter Terms of Service, which were updated on May 17, 2012. Those Terms of Service incorporate two documents by reference: Twitter's Privacy Policy (also updated on May 17), which notes that use of Twitter's services constitutes consent to the collection, transfer, manipulation, storage, disclosure, and other uses of information described in such policy, and the Twitter Rules, which describe how end-users should and should not use Twitter, and impose a variety of rules regarding content, spam and abuse. But the Terms of Service also link to Twitter's Developer Rules of the Road (described by Twitter as "an evolving set of rules for how ecosystem partners can interact with your content"), which govern the use of Twitter's application programming interface (API) and, more generally, Twitter's philosophy around how information and content shared on Twitter can and cannot be used. (If you'd like to review Twitter's latest Terms of Service and Privacy Policy revisions, please visit this link.)

Be sure to carefully review each social media service's terms and conditions so that you know what you are getting into, particularly when you will be investing money or time in using such service for your business or building an app or site that relies on the service's content or functionality.

Given the complexity of Twitter's ecosystem, the Developer Rules of the Road branch off to and incorporate a variety of other policies and guidelines, including the service's Display Guidelines (which describe how Tweets must be displayed), rules on trademark usage, automation rules, spam rules (which actually loop back to the end-user-focused Twitter Rules), and various other documents. Twitter's "Report a Violation" page includes the Twitter Rules and nearly 40 other policies, guidelines and related documents, all in addition to Twitter's Terms of Service, Privacy Policy, Developer Rules of the Road and other core documents.

Below, we describe a few key terms from Twitter's various written policies. These terms are not necessarily uncommon for Internet-based services – particularly services that are free to use – but they're worth keeping in mind:

Key Term for End-Users – Broad License to User Content. Foremost for many *end-users* of social media services, is the license being granted to such services in users' posted content – and end-users grant Twitter a typically broad license. By posting photos or other content on any of Twitter's services, end-users grant Twitter the right to "use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute" such content in any manner now known or later developed. The Terms of Service also expressly provide that such license "includes the right for Twitter to provide, promote, and improve the Services and to make [such content] available to other companies, organizations or individuals who partner with Twitter" for the purpose of distributing such content on other media and services. True, given that Tweets are publicly available by their nature (assuming a public account), one would expect a broad license grant. But the grant to Twitter gives Twitter the right to use Tweets for purposes other than simply operating the Twitter service, and the right to distribute those Tweets in ways that may not have even existed when the Tweets were originally posted. Although the broad license grant does apply to "protected" Tweets (i.e., Tweets that are not publicly viewable) and public Tweets alike, Twitter does state that protected Tweets will not appear in Twitter or Google searches, meaning that, as a practical matter, a user's privacy settings

should be useful in controlling how widely Twitter may disseminate the user's Tweets.

Key Terms for Developers – API Terms. Foremost for many *developers* who leverage social media services, are the services' rules for accessing their platforms and APIs. According to Twitter's Terms of Service, unless otherwise permitted through Twitter's services or through its Terms of Service or Developer Rules of the Road, users are required to use the Twitter API in order to "reproduce, modify, create derivative works, distribute, sell, transfer, publicly display, publicly perform, transmit, or otherwise use" Twitter's content or services. In light of this, it is important for developers who leverage Twitter in their own apps and services to carefully review the terms and conditions governing Twitter's API. Those terms and conditions are sprinkled throughout Twitter's policies, including the Developer Rules of the Road (changes to which are archived at Twitter's API Terms of Service Archive) and Twitter's Rate Limiting page, which addresses the number of "calls" that can be made to various Twitter APIs and services over time. Of course, all of Twitter's API restrictions are in addition to, and not in lieu of, those found in the site's Terms of Service and elsewhere; per the Developer Rules of the Road, use of the API and Twitter content "are subject to certain limitations on access, calls, and use as set forth in the [rules], on dev.twitter.com, or as otherwise provided to you by Twitter." Perhaps most importantly, Twitter retains the right to block use of the API and Twitter's content if Twitter believes that a user has attempted to circumvent or exceed any limitations imposed by Twitter, and Twitter disclaims any liability for resulting costs or damages.

Key Terms for Everyone – Modifications to Twitter's Terms and Services. Twitter reserves the right to unilaterally modify its Terms of Service and the form and nature of its services at any time. If Twitter determines in its sole discretion that changes to its Terms of Service are material, Twitter promises to notify users via a Twitter update or by email; nevertheless, as with changes to most websites' terms of use, a user's continued use of Twitter following such changes constitutes the user's agreement to the modified terms. It is important to keep in mind that changes in a social media site's services or terms of use – even seemingly tiny changes in the way a social media profile appears to end-users, or in what flavors of activities are or are not permitted on the site – can wreak havoc on a company's costly social media strategy. Conveniently, Twitter provides an archive of previous versions of its Terms of Service, which can help users spot changes over time more easily.

Our message to end-users and developers alike remains what it was back in 2010: be sure to carefully review each social media service's terms and conditions so that you know what you are getting into, particularly when you will be investing money or time in using such service for your business or building an app or site that relies on the service's content or functionality.

Status Updates

Online democracy in action? Facebook has announced that it will allow its 900 million plus user community to vote on proposed changes to its Statement of Rights and Responsibilities and its Privacy Policy. The results will be binding on Facebook if more than 30% of all active registered users cast votes; otherwise, the vote will be advisory. The polls close on June 8, 2012, at 9 AM PT.

Put a pin in it: Red-hot social media company Pinterest reportedly has been embroiled in lengthy and contentious negotiations with Getty Images over copyright issues raised by Pinterest's controversial business model. Getty is reportedly seeking to have Pinterest use Getty's PicScout image detection software, presumably to help police against unauthorized uses of third-party images in connection with Pinterest's site.

Well, what did you expect? In *Ehling v. Monmouth Ocean Hospital Service Corp.*, the U.S. District Court for the District of New Jersey waded into the murky waters surrounding reasonable expectations of privacy in not quite public — but not exactly private either — Facebook pages. The court held that a hospital supervisor who accessed an employee's Facebook page, allegedly by coercing one of the employee's Facebook friends, may have invaded the employee's privacy under New Jersey common law. The court noted that "[p]rivacy in social networking is an emerging, but underdeveloped, area of case law."

According to a settlement announced by the Federal Trade Commission, MySpace has agreed to settle claims that it misled users about its privacy policies and made false statements regarding its compliance with the U.S.-E.U. Safe Harbor privacy principles. Among other things, the proposed settlement would subject MySpace to privacy reviews for the next twenty years.

Apparently the road to getting a DMCA Section §512(f) complaint dismissed is paved with good intentions, at least according to the U.S. District Court for the District

of Montana. In *Ouellette v. Viacom International Inc.*, the court held that the plaintiff needed to allege a factual basis for his argument that defendant Viacom knew his YouTube videos qualified as fair use in order to pursue a wrongful DMCA takedown notice claim under Section 512(f) of the DMCA.

Make sure to read this case the next time you are planning to buy a truckload of socks online. The New York District Court for Nassau County held in *Jerez v. JD Closeouts, LLC* that a dispute between a New York plaintiff and a Florida "closeout" specialty vendor involving the purchase of thousands of pairs of tube socks was not subject to a forum selection clause that was "submerged" on the vendor's webpage and only accessible through an inconspicuous link.

Updating an allegedly defamatory article posted on a newspaper's website by adding "like" and "share" buttons did not constitute a republication for purposes of New York's one-year statute of limitations for defamation claims, according to the New York state court in *Martin v. Daily News LP*. The court rejected the plaintiff's argument that, by adding the buttons, the defendant provided new ways for the article to be distributed and intended to reach a new audience.

President Obama took to Twitter on May 23, 2012 for a "mini town-hall," bringing 140-character governance — and campaigning — to the people and responding directly to citizens' questions. Contrast this to the President's 2011 Twitter Town Hall, where questions were limited to journalists. Although the impact of events such as these, even when presidential, is open to debate, the Q&A points up the importance of one-to-one digital engagement in any business, including the business of government. (We were hoping for a Twitpic of the President's lunch coupled with an "OMG this pizza is AWEsome!! #DoublePepperoni" status update. No such luck.)

With nearly one in every seven people on the planet already a member of Facebook's user community, where to look for future growth opportunities? *The Wall Street Journal* reports that Facebook is contemplating a plan to allow kids under the age of 13 to use its social media platform under their parents' supervision.

The parties' proposed settlement having been rejected last year, Google has suffered yet another setback in the long-running litigation over its controversial book scanning project -- the court has granted class action status to authors pursuing copyright infringement claims against Google.

In some positive legal news for Google, a French court has sided with Google-owned YouTube in a copyright infringement suit arising from YouTube's hosting of infringing user-generated videos. According to press reports, the court found that YouTube had no obligation to control or filter content uploaded to its site by others. The court did note, however, that, once a copyright owner makes YouTube aware of the presence of infringing content on YouTube's site, YouTube would be responsible for taking steps to remove such content. *The New York Times* reports that there is now a growing body of cases in Europe addressing YouTube's potential liability exposure with respect to user-generated content.

The National Labor Relations Board's Office of General Counsel has issued its third report providing guidance to employers regarding employee-directed social media policies. We will be preparing a summary of the report for our next issue of *Socially Aware*, but, if you can't wait, a copy of the report can be found here.

Microsoft publicly launched its "So.cl" social media site in May 2012. According to Microsoft, So.cl is an experimental research project powered by Microsoft's Bing search engine that "lets you use search to express and share ideas through beautiful story collages." Story collages are generated from among the results of Bing searches made while logged in to the service. Users can add standard comments to So.cl posts, but they can also "*riff*" -- a riff spawns an entirely new post that's linked to but separate from the old one, thereby growing the collage and the conversation. So.cl also offers the ability to create shareable collections of videos called "video parties." We'll keep you posted as these new functionalities enter the social media lexicon and So.cl becomes more...social.