CENTER FOR JUSTICE & DEMOCRACY
CJ&D
at NEW YORK LAW SCHOOL

IMPACT

Spring 2015
Volume 14, Issue 2

...news, views and reviews from the Center for Justice & Democracy

CENTER FOR JUSTICE & DEMOCRACY **NEWS**

Dear Friends,

CJ&D is growing! We just hired a new Assistant Director, a brand new position at CJ&D. She's a fantastic New York Law School grad by the name of Nicole Reustle, and she comes to CJ&D with a very impressive background: political campaigns, legislative advocacy and plaintiffs' work. We're know you'll be seeing great things from Nicole.

We're so excited to be expanding our staff and we thank all of our supporters for that. We're working hard. From speaking before two federal agencies in the past month (the Consumer Financial Protection Bureau and the Food & Drug Administration), to writing major studies like our class action report (just entered into the record of a recent congressional hearing), to producing our shorter, easy-to-read Huffington Post pieces, PopTort blogs and Spotlights on Justice (see our website), to helping fight state and federal battles in innumerable ways, we have more than enough work to keep us very busy these days.

With Nicole coming on as a great new addition to our staff, there's no limit to what we can accomplish. OK, there may be some limits. But just try to stop us!

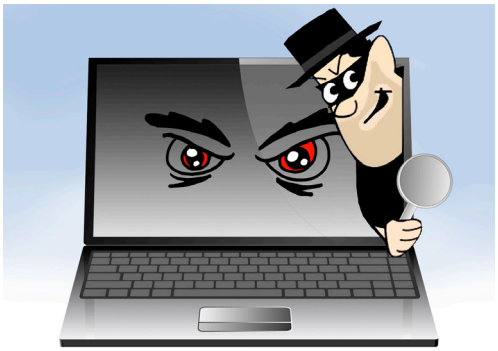
Sincerely,

Joanne Doroshow
Executive Director

IN THIS ISSUE: ONLINE PRIVACY

PRIVACY PROBLEMS IN NEED OF SOLUTIONS

New technologies, especially the Internet, have brought extraordinary benefits to consumers' lives. Yet the more we access the cyber world for products, services, information and entertainment, the more our privacy is in jeopardy. As we shop, pay bills, even view our medical records on computers and other web-enabled devices, companies are tracking, collecting, using, storing and sharing massive amounts of data about us, usually without our knowledge or consent.



Unfortunately, this insidious, unprecedented shift in consumer data control, access and profiteering has not been met with any meaningful privacy oversight from the federal government. The Federal Trade Commission (FTC) is charged with protecting the privacy of consumers' personal information but its enforcement efforts are primarily reactive, with the agency unable to keep up with the frequency and scope of consumer privacy rights violations that have become standard business practice for countless Internet service providers (ISPs), websites and other online services. The FTC's enforcement activ-

(continued on page 2)

THE INTERNET OF THINGS

The "Internet of Things" (IoT) refers to the ability of everyday objects – cameras, baby monitors, TVs, home security devices, fitness monitors, household appliances, cars, health trackers, etc. – to connect to the Internet and send and receive data. According to a January 2015 FTC report, "The sheer volume of data that even a small number of devices can generate is stunning," where "fewer than 10,000 households using [one] company's IoT home-automation product can 'generate 150 million discrete data points a day' or approximately one data point every six seconds for each household," for example.

The pace of this technology wave is equally staggering, with many anticipating the "Internet of Everything." "Six years ago, for the first time, the number of 'things' connected to the Internet surpassed the number of people," explained the FTC study. "Yet we are still at the beginning of this technology trend. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion."

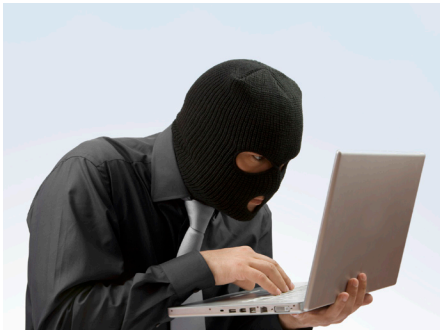
True, the IoT offers many benefits to consumers, such as managing health-

(continued on page 3)

ity is also inconsistent, triggered by privacy violations the agency deems unfair or deceptive vis-à-vis the broad privacy policies that companies craft and promote. Moreover, the FTC usually can't issue civil fines. Though a recent Federal Communications Commission (FCC) vote may shift the FTC's privacy enforcement jurisdiction over ISPs to the FCC – which would then have the power to require ISPs to obtain customers' consent before monitoring or sharing their personal information – it's questionable whether "the change survives the legal challenges that are sure to follow," argued the February 27, 2015 *Washington Post Switch Blog*. Nor does transferring some enforcement power tackle the larger issue of the FTC's inability to stem the rampant practice and proliferation of illegal consumer data appropriation by online companies.

The Obama administration's attempts to spearhead comprehensive consumer online privacy protections have been disappointing. In February 2015, the White House released a long-awaited draft of consumer privacy legislation that gives companies even more power to set their own rules. As explained in a February 27 joint statement from U.S. Reps. Frank Pallone (D-NJ) and Jan Schakowsky (D-IL), the proposed Consumer Privacy Bill of Rights Act is rampant with anti-consumer provisions. For example, it "encourages a self-regulatory system that could allow companies to design the privacy policies the FTC would enforce. Based on that model, all current practices related to data collection, use, and sharing – even flawed practices – would be allowed to continue." Federal panelties would be minimal, and "state laws designed to hold companies accountable for protecting their customers' personal information would be preempted, and individuals would be prevented from pursuing legal action if privacy policies are violated."

The proposed legislation was met with immediate and widespread criticism.



"When I look at it as a whole, I am disappointed with the starting point for the discussion," FTC Commissioner Julie Brill told the *Pittsburgh Post-Gazette*. "One of the fundamental problems I have with the way I think the whole bill would work is there seems to be very little of a bottom line." "No bill at all would have been better than this one, which would effectively codify bad behavior," argued a March 6 *New York Times* editorial. Even industry groups like the Internet Association – whose members include Amazon, AOL, Facebook, Google, LinkedIn, Netflix, Twitter, Yahoo!, Yelp and a host of other huge online consumer companies – called the bill a "wide-ranging legislative proposal" that "casts a needlessly imprecise net."

In the meantime, Sens. Ed Markey (D-MA), Richard Blumenthal (D-CT), Sheldon Whitehouse (D-RI) and Al Franken (D-MN) have introduced the Data Broker Accountability and Transparency Act (S. 668), which would give consumers the ability to access and correct sensitive personal information collected and sold by data brokers. The bill, supported by the FTC and consumer groups, also empowers consumers to bar such companies from using, sharing or selling their personal information for marketing purposes and gives the FTC the authority to enforce the law and promulgate rules.

On the state level, few legislatures have taken steps to fill the consumer Internet privacy void left by Congress and the White House. California has been a leader in this area, requiring commercial website and online service operators that collect personal data on state residents to adhere to their own privacy policies, which must be detailed as to collection, sharing and tracking practices and conspicuous to consumers. The state also bars online educational service operators from selling student data as well as using such data for targeted advertising

(continued on page 3)

CENTER FOR JUSTICE & DEMOCRACY
CJ&D
at NEW YORK LAW SCHOOL

185 West Broadway
New York, NY 10013
Phone: 212.431.2882
centerjd@centerjd.org
http://centerjd.org

IMPACT

Editor:
Daniel Albanese

Written By:
Emily Gottlieb

PRIVACY PROBLEMS IN NEED OF SOLUTIONS continuted…

or other non-educational purposes. Minnesota and Nevada are other examples, prohibiting ISPs from disclosing personally identifying information without customer approval, with Minnesota also requiring subscriber permission before ISPs can disclose customers' online surfing habits and website visit histories. Yet the small patchwork of these and other state-led initiatives can only go so far in combatting our national consumer online data privacy problem.

Some consumers have taken matters into their own hands and filed lawsuits to hold online companies accountable for unpermitted appropriation and use of their personal data. These civil cases, brought as individual lawsuits or class actions, have exposed unconscionable business practices that cross the privacy line. For example, in November 2013 court filings related to a proposed class action lawsuit, Google admitted that it opens up, reads and acquires the content of users' private email messages. "Just as a sender of a letter to a business colleague cannot be surprised that the recipient's assistant opens the letter, people who use web-based email today cannot be surprised if their communications are processed by the recipient's [Electronic Communication Service] provider in the course of delivery," Google asserted. The company also stated that it scanned the content of millions of student emails for non-

educational ad-targeting purposes, even when schools turned off the ability to display ads.

So what's the solution? Unfortunately there's no silver bullet, but a stronger, comprehensive policy from the White House, federal agencies and Congress is essential.

THE INTERNET OF THINGS continuted…

care at home, more efficient home energy use and real-time vehicle diagnostics that can result in safer highways. Yet at the same time such increased connectivity creates significant risks to consumer security, even more than those presented by mobile phones, tablets and traditional computers since, according to the FTC, "companies entering the IoT market may not have experience in dealing with security issues" related to the collection, transmission, storage and sharing of sensitive personal data, plus many IoT devices are inexpensive and "essentially disposable," making software security updates difficult, impossible or non-existent.

Consumer privacy in the IoT world is also a pervasive problem, with devices and sensors enabling "direct collection of sensitive personal information, such as precise geolocation, financial account numbers, or health information" as well as "the collection of personal information, habits, locations, and physical conditions over time, which may allow an entity that has not directly collected sensitive information to infer it," the FTC reported. Companies can then use these data to bar access to credit, insurance or employment.

Despite the above findings, the FTC has decided not use its recent report as a call for heightened federal policing of corporate security and privacy practices regarding IoT devices sold to or used by consumers. In contrast, U.S. Sens. Blumenthal and Markey are pointing to key discoveries in Markey's February 2015 report, *Tracking & Hacking: Security & Privacy Gaps Put American Drivers* at Risk, as proof that the nation needs federal legislation to protect the data, security and privacy of drivers in Internet-connected vehicles. "There are currently no rules of the road for how to protect driver and passenger data, and most customers don't even know that their information is being collected and sent to third parties," Markey explained in a February 11 press release. "These new requirements will include a set of minimum standards to protect driver security and privacy in every new vehicle." "Connected cars represent tremendous social and economic promise, but in the rush to roll out the next big thing automakers have left the doors unlocked to would-be cybercriminals," added Blumenthal. "This common-sense legislation would ensure that drivers can trust the convenience of wireless technology, without having to fear incursions on their safety or privacy by hackers and criminals." Hopefully this federal action will just be the beginning of things when it comes to protecting consumers from IoT privacy and security vulnerabilities.

Medical history, credit card numbers, bank account balance, first and last name, passport number, date of birth, Social Security number. Personal information is among our most valuable possessions. It's also data that we expect to be protected, even when it goes into corporate hands. Yet time and again, Americans' sensitive personal data is stolen because companies don't have cyber safeguards in place. Just look at the daily headlines – "JPMorgan: 76 million customers hacked," "Home Depot breach exposes a whopping 56M credit cards," "Anthem says at least 8.8 million non-customers could be victims in data hack," "Sony Breach May Have Exposed Employee Healthcare, Salary Data," "Michaels confirms breaches exposed nearly 3M credit cards," "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," "Experts warn 2015 could be 'Year of the Healthcare Hack,'" the list goes on and on.

Empirical evidence tells the same story. "In 2014, over 68 million records were exposed by data breaches in the business sector and more than 8.2 million records were exposed by data breaches in the medical/healthcare industry (which includes insurance companies)," according to a 2014 Identity Theft Resource Center (ITRC) report.

For large corporations, the costs of consumer data breaches are minimal, leaving companies with little incentive to strengthen their cybersecurity. Aside from temporary reputational damage, big companies often leave massive consumer data breaches unscathed. Federal and state law-enforcement agencies are not only woefully underfunded and understaffed but also don't have enough policing power at their disposal. For example, as of publication, the 3rd Circuit is deciding whether the FTC can sue companies over cybersecurity practices that compromise consumer information. In *FTC v. Wyndham Hotels & Resorts*, the agency alleges that Wyndham not only misrepresented its security practices vis-à-vis consumers' personal information but that such cybersecurity lapses led to repeated large-scale breaches, resulting in "fraudulent charges on consumers' accounts, millions of dollars in fraud loss, and the export of hundreds of thousands of consumers' payment

card account information to an Internet domain address registered in Russia," according a June 2012 FTC press release. Ruling against the FTC could seriously undermine the FTC's ability to bring cases against companies that fail to safeguard consumer data. As former FTC Director of Consumer Protection David Vladeck explained in the *WSJ*'s March 3 *Risk & Compliance Journal* blog, dismissing the agency's case would "leave a vast area of the law without a regulatory authority," forcing states to take up the data security mantle.

Big companies also lack any financial incentive to take consumer data security more seriously. "When we examine the evidence," Columbia University Internet governance and cybersecurity fellow Benjamin Dean wrote in a March 4 article published on *The Conversation website*, "the actual expenses from the recent and high-profile breaches at Sony, Target and Home Depot amount to less than 1% of each company's annual revenues. After reimbursement from insurance and minus tax deductions, the losses are even less." Based on these numbers, Dean concluded, "[i]t therefore does not make economic sense for companies like Home Depot to make large investments in information security. As a result, they do not."

Moreover, industry has the ear of the Obama administration and federal lawmakers, who, instead of focusing on protecting consumers, have turned their attention to business-backed legislation that shields companies from lawsuits for sharing cyberthreat information with the government. As for the states, NYS Attorney General Eric Schneiderman recently proposed corporate law firm-endorsed legislation that would allow companies to eliminate all liability if they adopt a heightened level of data security or share forensic reports with law enforcement officials after a data breach occurs. "We must also remind ourselves that companies can be victims, and that those who take responsible steps to safeguard customer data deserve recognition and protection," Schneiderman said in a January 15, 2015 press release.

Immunity would be a mistake. With the cybersecurity discourse focused on business losses and consumers insufficiently protecting their personal information, class action lawsuits are important. Such lawsuits enable data breach victims to come together to seek justice and compensation for similar harm where individual lawsuits would be impossible. Class actions can also provide an incentive for unprepared corporations to rethink their practices and procedures and put other companies on notice that they can be held accountable for similar negligent or reckless behavior. In addition, such suits can alert unwitting victims about businesses' cybersecurity practices that can or may have already jeopardized their health and safety.