THE ADVOCATE
Santa Clara University School of Law
School of Law Newspaper Since 1970
Thursday, October 15, 2015
Volume 46 Issue 2

HTLI Hosts “Privacy Crimes: Definition and Enforcement”

By Brent Tuttle
Editor-in-Chief

On October 6th, SCU Law’s High Tech Law Institute, the Markkula Center for Applied Ethics, and the Santa Clara District Attorney’s Office hosted the first ever “Privacy Crimes: Definition and Enforcement” half-day conference. The Electronic Frontier Foundation (EFF), the International Association of Privacy Professionals (IAPP), and the Identity Theft Council (ITC) also sponsored the free event. It brought together practitioners, academics and students to discuss several important questions that both civil and criminal legal professionals face in the digital age. For example, what is a privacy crime? What is being done to enforce the laws addressing these privacy crimes? Furthermore, how can we balance privacy interests in the criminal justice system?

After opening remarks from Santa Clara District Attorney Jeffrey Rosen, Daniel Suvor gave the keynote address. Mr. Suvor is the Chief of Policy to the Attorney General of California, Kamala Harris, and former Senior Director of the Office of Cabinet Affairs at the White House. Mr. Suvor discussed his work with the California Attorney General’s Office and elaborated on the AG’s stance regarding the current state of privacy crimes.

Mr. Suvor spoke of the California AG’s efforts to combat cyber-crimes. He noted that California was the first state to have a data breach notification law, implemented in 2003. Mr. Suvor also discussed a recent settlement between the CA Attorney General and Houzz, Inc. that is the first of its kind in the United States. Among other things, the terms of the settlement require Houzz, Inc. to appoint a Chief Privacy Officer who will oversee the company’s compliance with privacy laws and report privacy concerns to the CEO and/or other senior executives.

The California Attorney General has also increased privacy enforcement through the creation of an E-Crime Unit in 2011 to prosecute identity theft, data intrusion, and crimes involving the use of technology. To date, the E-Crime Unit has conducted several investigations involving piracy, shutting down illegal streaming websites, and online counterfeit operations. Mr. Suvor noted a recent area of priority to the Unit: the prosecution of cyber exploitation, commonly known as “revenge porn.”

Mr. Suvor clarified that the AG’s Office adamently believes the term “revenge porn” is a misnomer. The Office takes the position that cyber exploitation is more appropriate for two reasons. First, porn is generally created for public consumption, whereas “revenge porn” was not created with a public audience in mind. In addition, the Office does not give any credence to the notion that the publisher of non-consensual porn has any legitimate interest in vengeance.

See Page 5 “Privacy Crimes Continued...”

SCU Law Student Showcases Origami with on-Campus Exhibit

By Flora Kontilis
Staff Writer

While I thought it was a logical prerequisite, he doesn’t fold paper airplanes. “I never mastered the skill,” says 3L Trevor Mead. Even so, he doesn’t fall short. Ironically enough, Mead is a bona fide origami artist, creating anything from koi fish made from dollar bills, to a true-to-size horse made from an 18-foot by 18-foot sheet of paper – a project that took nearly seven hours to complete. Yet you probably recognize Mead’s more recent work: life-sized origami sheep that dotted the Santa Clara University Mall.

“So many people asked what the sheep were saying about the law school and its students!” Mead recalls from his daytime exhibition. “Their sole purpose is to delight. That’s it! Anything more is projecting [and revealing] what the viewer wants,” he says. Fair enough. But what does Mead want? What’s the takeaway from giant origami? To him, the sheep “are a reminder how much there is to life outside of law school.” So the “big picture” message is an invitation to take a step outside of that space. Ultimately, Mead’s craft is about finding “work-life balance. I’m passionate about protecting this,” he states.

A Denver native, Mead’s legal interests focus on privacy law and copyright licensing for independent artists. He boasts a strong academic and professional resume: while earning a Privacy Law Certificate through the High Tech Law Institute, he has worked in the privacy industry for almost two years as an intern at TRUSTe. Prior to law school, he pursued a career in sales, simultaneously providing business and technology consultation services for over six years in Denver.

How does giant origami come into this? According to Mead, “it’s a very complimentary hobby to law, because it’s nothing but an exercise in precision, concision and perseverance. If that doesn’t describe what we are doing in law school, then I don’t know what does.” For instance, consider folding koi fish, a special subject to Mead. It was his first complex dollar-bill fold, one he later scaled-up into giant wall art during his 11 year. The project took 15 hours to fold, ten of that dedicated to tedious pre-creasing to form the basis of the design.

Yet, looking at Mead’s impressive professional and academic background, his craft comes back to finding work-life balance. For Mead, giant origami is a “very Zen activity”; one that comes down to “protecting personal time by refusing to let go of that part of myself, despite the pressure from law school.”

In addition to consistently promoting this idea of fostering “you-ness,” Mead admits there’s more to giant origami than just the final product: “what I love about origami is its transient nature – creating something and releasing it into the world, knowing it will fade away. It’s a personal meditation on acceptance and release.”

On that note, Mead’s art is both solitary and social. He remembers setting up in Boulder’s Pearl Street Mall, a familiar stomping ground in Colorado, where he would “just start folding. It was a great way to talk to people, offer a glimpse into the artistic process, and provide a sneak peek of the next big project,” Mead recalls.

While he enjoys talking with and meeting different spectators, Mead also finds inspiration from fellow artists—especially, as Mead points out, since the art has advanced significantly in the last 20 years. Technology has transformed origami in unprecedented ways, a selling point for Mead. “There’s an entirely new level of complexity! New designers are developing and mastering new techniques,” he says. To stay current with modern trends, Mead joined a local maker space that serves as a communal workshop, with access to anything from laser cutters, to 3D printers, CNC routers, and more. Mead says of the maker space, “it’s where you turn ideas into product. The space provides the inspiration and tools necessary to get there.”

Even as Mead脾胃s new resources to make leaps and bounds in origami art, he reminds me that it’s not about being an expert. Rather, in the same spirit he approached law school, he finds it motivating to be around like-minded beginners. “Regardless of what we did before, we’re all novices here,” Mead says. “It’s refreshing to be a novice again.”

As he continues, Mead emphasizes the value of peers to collaborate with and to support on this professional journey. This concept ties closely with artistry. Mead elaborates, “creativity is not an innate skill. It’s learned, like anything else; it’s only a question of whether you choose to cultivate it or not.”
De Cuba.

The general rule of property law in Cuba is that the state owns all property, real or personal, or as the Constitucion says, all property is “socialist state property which is the property of the entire people.” As we see with most laws, the general rule is subject to a number of exceptions. The Constitucion allows for private ownership rights of intellectual property; private companies as a rule are subject to a number of exceptions. The Constitucion further allows for ownership of small farms and cooperatives, but no land leases or mortgages on such lands, or any acts which permit the use of state property which is the property of the entire people. Before going into this month’s rumor, can I just put in a plug for the last edition of the Rumor Mill? Own It! Own your behavior at the Halloween Bar Review? Own your appropriate and modest costume! Own your reputation . . . (see below) Dear Rumor Mill. Just a couple of months after raising our hands and pledging to be ethical and honest, we had SBA class rep elections. I’ve heard rumors about students who were stealing treats and other tools of bribery from each other and co-opting them for their own campaign. They were also defacing each other’s campaign material. Can they get expelled for this dishonest behavior? Thanks for the note. I have a couple of responses. First, I will check in with the SBA leadership and see if they were aware of these issues. We think it’s important that student organizations be run by the students. You can’t learn to be Lawyers who Lead if you never get to be in charge. We have a graduate who is now legal counsel at a local startup, who used to come back every year and talk to our students about his experiences as a new lawyer. Jeff would share how in his first job interviews, when asked to talk about his experience, he could share stories about how he resolved conflicts between students, how he organized large ski trips and community service experiences and how he motivated students to get involved. He talked about how, in his first few years on the job, he relied on the lessons learned as a leader of students to make daily decisions. This is all good stuff. If things go well, you learn something. If things go badly, you probably learn more. If people lie and cheat, you learn a lot about them as individuals. So, since this is an SBA issue, we would leave it to them to figure out what to do. This issue also opens up the opportunity for me to say again that your reputation starts now. Stealing someone’s cupcakes and passing them off as one’s own may seem minor, but maybe it’s a glimpse into what a person thinks is funny or acceptable. Maybe people are a little more careful around the cupcake thief - - who’s to say that your twinkies won’t be next?!? What if the poster defacer is in court one day and the opposing counsel is the victim of the graffiti in question? As a lawyer, your career will be made or broken based on your reputation. Protect it! OWN IT! And the last thing I will say on this topic is please be kind to each other. We are a community. Like it or not, these are your people. Be nice to your people. We all have our own challenges and problems. Real life happens and it can be a real beast. Law school doesn’t always leave you a lot of free time to deal with everything else in the world. At least here at the law school, your people understand what you are going through. At least here, we should understand that sometimes our classmates could use a little bit of understanding or support or just a little bit of kindness. We support each other at SCU. We don’t steal from each other, we don’t undercut each other. We need to respect and care for each other. Please be nice to your people. If you or someone you know needs help, please walk them up to see us in Student Services or walk them over to Cowell Health Center to make an appointment with a counselor. Talk to a professor. Talk to your people. And remember . . . we are your people.

Heard any rumors lately? If so, send me an email – servin@scu.edu
By Stephanie Brit
Staff Writer

On September 9th, New York Supreme Court Justice Allan Weiss ruled that the electronic-hails utilized by rideshare apps such as Uber and Lyft are legal despite NY Taxi's claims that they create unfair competition. This ruling has effectively rendered the $10 billion industry behind taxi's gold medallions worthless. Justice Allan Weiss wrote, "Any expectation that the medallion would function as a shield against the rapid technological advances of the modern world would not have been reasonable, in this day and age, even with public utilities, investors must always be wary of new forms of competition arising from technological developments."

While it is refreshing to see that the country still upholds the values of a free-market economy, it also brings to question many other issues regarding the surge in rideshare programs. It is argued that permitting e-hails rather than the iconic whistle to hail a cab simply acknowledges that the industry must adapt to recent technologies, however, there are considerable consequences that are not being addressed by the courts.

It is both imperative and ironic that current ride-share apps have utilized the development of technology to provide transportation services without owning a single car. The fact that companies such as Uber and Lyft can provide transportation without any of the traditional overhead costs of purchasing a vehicle, imposing background checks on drivers, or the recurring costs of maintaining the vehicles leads to a business model that is highly profitable. Despite the minimal risk that the companies face in their investment in the ride-share sector, there is also the question of whether the free-market approach toward these services reckless disregards the rights that employees and clients should be entitled to. Does the protection of free-market ideals ultimately lead to the exploitation of the drivers? In addition, does the increased accessibility into the ride-share market result in passengers putting themselves at greater risk each time they get into a car for the sake of saving a few dollars?

I asked an Ethiopian taxi driver what he thought about the recent surge of apps such as Uber and Lyft and whether he was considering trading in his taxi medallion for the pink moustache. He laughed at the idea, "It is not worth it. I came to this country in order to work and find a better life. With Uber and Lyft, you never know whom you're going to pick-up, but with taxis, the medallion provides the protection in case of an incident. Any kind of profit is not enough to lose that kind of protection." The overhead costs of taxi companies pay for the necessary costs in providing insurance for the vehicles. When I got into my Uber driver's Toyota Camry, I asked him whether Uber helped to pay for maintenance costs. He shrugged, "No, no, I have to pay those costs myself. I pray I don't break down because I need to work." It is clear from this that the benefits of driving for ride-share programs are popular among customers for the affordability, but that the risks for drivers are too great to be profitable in the long-term.

As a student without a car, cheap ride-share programs are incredibly convenient for me, but the fact is that you never know whose car you're boarding. Getting into a car with a stranger certainly puts up some red flags. A recent Lyft driver and I bonded over our favorite Persian restaurants during the ride and at the end of the ride he offered me his number to go grab Kabob's for lunch. As well intentioned as I hope the gesture to be, I realized that there is a significant risk for passengers that choose to get into the vehicles from companies that do not account for the security of their passengers. My concerns with New York's ruling in favor of e-hails is that the convenience and anonymity provided by ride-share apps caters towards reckless business practices.

Krebs also stated that our overwhelming reliance on static identifiers is the single biggest threat to privacy and security today. Using the IRS as an example, he presented a recent scenario, where 330,000 people were victims of tax identity fraud. The victims' information was obtained directly from the IRS website using the site's "Get Transcript" feature. This allows anyone to get an individual's previous tax returns using information such as date of birth, SSN and address. In addition, the site also required that the purported taxpayer answer knowledge-based authentication questions such as previous addresses, previous employers, or information relating to the worth of your house. The problem with these knowledge-based authenticators is that much of the information is readily available from sites such as LinkedIn, Facebook and Zillow. To date, the IRS admits that the fraudsters tried to steal roughly 660,000 taxpayer identities, meaning that through the static identifiers and knowledge based authenticators, they were successful in about 50% of their attempted heists. Because of this, Krebs considers these security authenticators a "joke."

However, he also stressed that these "knowledge-based" questions are the keys to accessing to services that are crucial to individuals' identities, credit reports, and retirement benefits. As a result of knowledge-based authenticators, Krebs believes that many protections for consumers actually backfire. The systems society relies upon to authenticate credentials are antiquated because all of this information is easily accessible on the web.

While Krebs was clear about his beliefs on information privacy, he concluded his speech by providing a few resources for those interested in attempting to protect their own. Here they are: Tor, Mullvad.net (VPN), DuckDuckGo (Browser), Ghostery (ad tracking blocker), GP+ Thunderbird (Email), Wickr (Mobile IM), Signal (iPhone call/text encryption), RedPhone (Android call/text encryption).
Office Hours Unwound

Michelle Oberman
Katharine & George Alexander Professor of Law
Areas of Specialization: Health Law

Education:
- J.D., University of Michigan Law School
- M.P.H., University of Michigan School of Public Health
- B.A., Cornell University

1. When was the last time you left the country? Where did you go and why?
   Last summer I spent a month working in El Salvador. It was my ninth visit in five years. I go, in part, because I'm writing a book about abortion and the law. Their law completely bans abortion, and given how we in the U.S. are embroiled in war over how the law should regulate abortion, it is interesting to see how the law does, and does not, work. I also go because of the volunteer work I get to do there. When I go, I stay in a village called Suchitoto. I live and work at the Peace Center for the Arts, a community center built and run by a U.S. born nun, Sister Peggy O'Neill. She's lived there for 35 years now. The Center is an oasis. On any given day, you might find: a chorus of trombones playing Ode to Joy; a convocation of the local teachers, organizing to petition the government for school supplies; or two muscular young men teaching Zumba to middle-aged women who've worked all day selling vegetables at the local market. I volunteer in the classrooms, making art or playing with the kids.

2. What was the most valuable course you took in law school and why?
   After being cautioned against it by many classmates, who warned that the class was too hard and the professor hated middle-class students (whatever that means), I took Health Law. It paved the path to my life's work, which is the intersection of health and law. My professor approached the subject by attending to the "forest" while insisting that we understand each tree at the most fundamental level. Even when class was confusing, it was the first time I didn't feel lost.

3. Who is your favorite character from literature and/or film?
   Professor McGonagall from Harry Potter.

4. What is your top source (news / journal / legal blog / other) for keeping current with the law?
   I still make a habit of reading the New York Times with my morning coffee and listening to NPR on my commute, but for keeping up with the law, I subscribe to various news feeds. Health law issues arise in a host of legal settings: politics, public health policy, ethics, business law, regulatory affairs, etc. I can't read everything and have a life. Chippling services have made things a whole lot more manageable.

5. What was your favorite job you had while in law school?
   I interned with the San Francisco Public Defender's Office. It provided me with valuable insight into how our criminal justice system worked, which has stayed with me and influenced my thinking about the criminal justice system and social issues in general.

6. What is your go to restaurant in the Bay Area? They are all in San Francisco, where I live. Rich Table is a favorite. I like Zuni Cafe and NOPA too.

7. What is your favorite show on Netflix, HBOGO, etc.? My favorites are The Walking Dead and the first season of True Detective (the second season really didn't deliver, right?). Also, The Fall, starting Gillian Anderson (from The X-Files), is excellent.

8. What is your favorite sports team? If no team, then do you admire a particular athlete and why?
   I love the Giants. I love baseball in general, and I love the scrappy way the Giants play it—or at least played it last year—as a team, rather than as a superstar (or two or three) plus the other guys.

9. What do you consider to be the most important development in your field over the last 5 years? This is too easy: The Affordable Care Act, (a.k.a. Obamacare) is the most significant legal development not only in health law, but in law, generally, since the 1960s. Built on our fragmented, complex and imperfect health care system, it is necessarily flawed. However, even in its first 5 years, it has already succeeded in increasing access to care for millions of Americans, while at the same time enhancing quality and reducing costs.

10. How do you unwind? In the pool. I swim until I'm no longer distracted by my jabbering thoughts. It doesn't take all that long, and it always makes me feel better.

Brian Mitchell
Founder of Mitchell + Company and Professor of Law
Areas of Specialization: Intellectual property litigation with an emphasis on patent, trademark, and copyright issues for technology clients

Education:
- J.D., University of San Francisco, School of Law
- B.S., California State University, Sacramento

1. When was the last time you left the country? Where did you go and why?
   The last time I was out of the country was a trip to Mexico City. I had just settled a case, and took advantage of a window of free time. I went for the restaurants and the museums, neither of which disappointed.

2. What was the most valuable course you took in law school and why?
   My practice is devoted to patent litigation, so obviously my courses on patents and patent litigation were very important. Also, a seminar course that I took from Thomas McCarthy, the trademark guru, was very influential towards my thinking about intellectual property law. Lastly, ethics. You would be surprised at how very influential towards my thinking about intellectual property law...and given how we in the U.S. are embroiled in war over how the law should regulate abortion, it is interesting to see how the law does, and does not, work. I also go because of the volunteer work I get to do there. When I go, I stay in a village called Suchitoto. I live and work at the Peace Center for the Arts, a community center built and run by a U.S. born nun, Sister Peggy O'Neill. She's lived there for 35 years now. The Center is an oasis. On any given day, you might find: a chorus of trombones playing Ode to Joy; a convocation of the local teachers, organizing to petition the government for school supplies; or two muscular young men teaching Zumba to middle-aged women who've worked all day selling vegetables at the local market. I volunteer in the classrooms, making art or playing with the kids.

3. Who is your favorite character from literature and/or film?
   Professor McGonagall from Harry Potter.

4. What is your top source (news / journal / legal blog / other) for keeping current with the law?
   I still make a habit of reading the New York Times with my morning coffee and listening to NPR on my commute, but for keeping up with the law, I subscribe to various news feeds. Health law issues arise in a host of legal settings: politics, public health policy, ethics, business law, regulatory affairs, etc. I can't read everything and have a life. Chippling services have made things a whole lot more manageable.

5. What was your favorite job you had while in law school?
   I interned with the San Francisco Public Defender's Office. It provided me with valuable insight into how our criminal justice system worked, which has stayed with me and influenced my thinking about the criminal justice system and social issues in general.

6. What is your go to restaurant in the Bay Area? They are all in San Francisco, where I live. Rich Table is a favorite. I like Zuni Cafe and NOPA too.

7. What is your favorite show on Netflix, HBOGO, etc.? My favorites are The Walking Dead and the first season of True Detective (the second season really didn't deliver, right?). Also, The Fall, starting Gillian Anderson (from The X-Files), is excellent.

8. What is your favorite sports team? If no team, then do you admire a particular athlete and why?
   I love the Giants. I love baseball in general, and I love the scrappy way the Giants play it—or at least played it last year—as a team, rather than as a superstar (or two or three) plus the other guys.

9. What do you consider to be the most important development in your field over the last 5 years? This is too easy: The Affordable Care Act, (a.k.a. Obamacare) is the most significant legal development not only in health law, but in law, generally, since the 1960s. Built on our fragmented, complex and imperfect health care system, it is necessarily flawed. However, even in its first 5 years, it has already succeeded in increasing access to care for millions of Americans, while at the same time enhancing quality and reducing costs.

10. How do you unwind? In the pool. I swim until I'm no longer distracted by my jabbering thoughts. It doesn't take all that long, and it always makes me feel better.
or revenge in carrying out such heinous acts. He noted that cyber exploitation also seeks to promote shame: and that California law expressly prohibits this conduct under California Penal Code, section 647. To tackle this problem, the Office is collaborating with the private sector. Mr. Fakhoury reported that Google, Facebook, Twitter, Reddit, and others have since adopted policies that will help victimize cyber exploitation.

Following Mr. Saver's keynote, Irvine Racine, Director of Communications for the Markkula Center for Applied Ethics, moderated a panel titled "What is a Privacy Crime?" The group of panelists consisted of Hanni Fakhoury, Staff Attorney at the Electronic Frontier Foundation; Tom Flattery; Santa Clara County's Deputy District Attorney, and Susan Friedland, a Professor at the University of San Francisco, School of Law.

Mr. Flattery opened the panel by acknowledging how hard it is to define a privacy crime. Privacy interests are amorphous. Some, to privacy is the right to be left alone. Others seek privacy in their communications, privacy in their autonomy; but depending on the individual, privacy expectation and concerns will vary. However, she drew a sharp distinction in differentiating privacy crimes from torts, because in this respect, the State has an interest in punishing an individual for privacy crimes.

Ms. Friedland also urged the audience that it is important to proceed with caution when defining privacy crimes. For example, she elaborated on the concern that people have notice of what exactly is illegal, what the appropriate level of culpability is, whether a privacy crime must be subjectively or objectively harmful, and that free speech may be an issue in courts. Furthermore, she urged that noticing people from privacy crimes could also confound our amendment. In this respect, she urged that we find a proper balance between protecting an individual's privacy while leaving room for freedom of speech and freedom of the press.

Mr. Flattery went into detail about the use of California Penal Code 502 to deal with privacy crimes. Specifically, section 502 contains anti-backing provisions that differentiate criminal activity by what an individual does with the data. For example, if someone merely gained unauthorized access to a social media or email account and did nothing with this data, then such a person would be subject to Penal Code 502(c)(7), though first offense is only a misdemeanor and an infraction, in the same vein as a speeding or parking ticket. However, if the individual used the information, then Penal Code 502(c)(4) (2) elevates the charge to a misdemeanor or felony. Mr. Flattery encouraged the audience to think about what the term "use" means in the context of the Code. Does this code section only apply when an individual uses the information to obtain financial gain, or does sharing this data with a group of friends also constitute a "use"? Mr. Flattery stated that questions don't really have "good clean answers" which leaves citizens without a bright-line rule in a context that will become increasingly more important over time.

Another area of concern Mr. Flattery highlighted was the increase of the use of medical IDs and electronic medical records. In these instances, people will go in to a hospital or medical treatment facility and assume the identity of someone else to obtain legitimate medical services under a stolen alias. However, as medical records increasingly become electronic, when the victim of this crime is a hospital or clinic under legitimate medical emergency, his or her electronic medical record is full of inaccurate medical information. In these cases, the identity theft can be life threatening, as a patient's record can incorrectly document that a wrong medication was administered to them.

Mr. Flattery highlighted the criminal liability of those seeking to employ medical records for revenge porn. Unless the victim is already aware of the identity theft, the identity the/ft can be life threatening, as a patient's record can correctly document that a wrong medication was administered to them.

Mr. Flattery also highlighted how the new law provides citizens with support for CalECPA, aka SB-178, which was signed by the Governor late last week. This new law provides citizens with privacy protections against law enforcement. Mr. Flattery distinguished this piece of legislation from others that might not be as robust. Mr. Flattery stated that these new laws did not address matters Mr. Flattery referred to as "commercial surveillance," where private companies use deceptive terms of service to illicitly collect data on their users.

Ms. Friedland shared her experience of the University and it's great for the public interest as a whole.

Mr. Flattery highlighted the fact that the privacy rights of the victim must be fairly weighed against the defendant's right to fully cross-examine and confront his or her accusers. And Mr. Fakhoury noted that the general identity theft statute is an applicable statutory remedy, so he questioned why we would need another law to handle this problem. Mr. Fakhoury also emphasized the potential issues of adding an abundance of new and different laws. New laws could be drafted sloppy or poorly and include ambiguous language that is left for courts to interpret, thereby covering more conduct than the proponent intended.

Mr. Fakhoury highlighted that if the records would have any relevance to the issue of search results still displaying content that has been taken down, it would allow for the Google and/ft to alter their practices to effectively tackle this problem. He described one case where a wrong medication was given to a patient and her mother spent 500 hours sending Digital Millennium Copyright Act takedown notices to websites. She also spoke on the need for the case to employ copyright takedown notices to websites. They described one case where a flight attendant was targeted by the defense sought psychological records and a retainer fee of $10,000. If the case goes to trial, the victim must pay $10,000.

Mr. Fakhoury shared his experience of the University and it's great for the public interest as a whole.

Mr. Flattery also emphasized that the information available to them is extremely valuable. Mr. Flattery suggested that the privacy crimes become more commonplace, the protections afforded to victims will be utilized as well.

The conference closed out with the panel "Balancing Privacy: Concerns in the Criminal Justice System," which was attended by approximately 70 attendees. In this presentation, the protection of privacy under the law still displays content that has been taken down, was "a real diversity of speakers and diversity of panelists consisted of Hanni Fakhoury, Senior Staff Attorney at the Electronic Frontier Foundation; Tom Flattery; Santa Clara County's Deputy District Attorney; Attorney Deborah Hernandez; and Ingo Brauer, a Professor at the University of San Francisco, School of Law.

Mr. Flattery emphasized the increasing the/ft of medical IDs and electronic medical records. In these cases, the identity the/ft can be life threatening, as a patient's record can correctly document that a wrong medication was administered to them. He noted that cyber exploitation also seeks to promote shame: and that California law expressly prohibits this conduct under California Penal Code, section 647. To tackle this problem, the Office is collaborating with the private sector. Mr. Fakhoury reported that Google, Facebook, Twitter, Reddit, and others have since adopted policies that will help victimize cyber exploitation.

Following Mr. Saver's keynote, Irvine Racine, Director of Communications for the Markkula Center for Applied Ethics, moderated a panel titled "What is a Privacy Crime?" The group of panelists consisted of Hanni Fakhoury, Senior Staff Attorney at the Electronic Frontier Foundation; Tom Flattery; Santa Clara County's Deputy District Attorney, and Susan Friedland, a Professor at the University of San Francisco, School of Law.

Mr. Flattery opened the panel by acknowledging how hard it is to define a privacy crime. Privacy interests are amorphous. Some, to privacy is the right to be left alone. Others seek privacy in their communications, privacy in their autonomy; but depending on the individual, privacy expectation and concerns will vary. However, she drew a sharp distinction in differentiating privacy crimes from torts, because in this respect, the State has an interest in punishing an individual for privacy crimes.

Ms. Friedland also urged the audience that it is important to proceed with caution when defining privacy crimes. For example, she elaborated on the concern that people have notice of what exactly is illegal, what the appropriate level of culpability is, whether a privacy crime must be subjectively or objectively harmful, and that free speech may be an issue in courts. Furthermore, she urged that noticing people from privacy crimes could also confound our amendment. In this respect, she urged that we find a proper balance between protecting an individual's privacy while leaving room for freedom of speech and freedom of the press.

Mr. Flattery went into detail about the use of California Penal Code 502 to deal with privacy crimes. Specifically, section 502 contains anti-backing provisions that differentiate criminal activity by what an individual does with the data. For example, if someone merely gained unauthorized access to a social media or email account and did nothing with this data, then such a person would be subject to Penal Code 502(c)(7), though first offense is only a misdemeanor and an infraction, in the same vein as a speeding or parking ticket. However, if the individual used the information, then Penal Code 502(c)(4) (2) elevates the charge to a misdemeanor or felony. Mr. Flattery encouraged the audience to think about what the term "use" means in the context of the Code. Does this code section only apply when an individual uses the information to obtain financial gain, or does sharing this data with a group of friends also constitute a "use"? Mr. Flattery stated that questions don't really have "good clean answers" which leaves citizens without a bright-line rule in a context that will become increasingly more important over time.

Another area of concern Mr. Flattery highlighted was the increase of the use of medical IDs and electronic medical records. In these instances, people will go in to a hospital or medical treatment facility and assume the identity of someone else to obtain legitimate medical services under a stolen alias. However, as medical records increasingly become electronic, when the victim of this crime is a hospital or clinic under legitimate medical emergency, his or her electronic medical record is full of inaccurate medical information. In these cases, the identity theft can be life threatening, as a patient's record can incorrectly document that a wrong medication was administered to them.

Mr. Flattery highlighted the fact that the privacy rights of the victim must be fairly weighed against the defendant's right to fully cross-examine and confront his or her accusers. And Mr. Fakhoury noted that the general identity theft statute is an applicable statutory remedy, so he questioned why we would need another law to handle this problem. Mr. Fakhoury also emphasized the potential issues of adding an abundance of new and different laws. New laws could be drafted sloppy or poorly and include ambiguous language that is left for courts to interpret, thereby covering more conduct than the proponent intended.

Mr. Fakhoury stated that these new laws would also protect the public by requiring law enforcement to get a search warrant beforehand. Mr. Fakhoury noted that the general identity theft statute is an applicable statutory remedy, so he questioned why we would need another law to handle this problem. Mr. Fakhoury also emphasized the potential issues of adding an abundance of new and different laws. New laws could be drafted sloppy or poorly and include ambiguous language that is left for courts to interpret, thereby covering more conduct than the proponent intended.

Mr. Fakhoury highlighted the fact that the privacy rights of the victim must be fairly weighed against the defendant's right to fully cross-examine and confront his or her accusers. And Mr. Fakhoury noted that the general identity theft statute is an applicable statutory remedy, so he questioned why we would need another law to handle this problem. Mr. Fakhoury also emphasized the potential issues of adding an abundance of new and different laws. New laws could be drafted sloppy or poorly and include ambiguous language that is left for courts to interpret, thereby covering more conduct than the proponent intended.

Mr. Fakhoury highlighted the fact that the privacy rights of the victim must be fairly weighed against the defendant's right to fully cross-examine and confront his or her accusers. And Mr. Fakhoury noted that the general identity theft statute is an applicable statutory remedy, so he questioned why we would need another law to handle this problem. Mr. Fakhoury also emphasized the potential issues of adding an abundance of new and different laws. New laws could be drafted sloppy or poorly and include ambiguous language that is left for courts to interpret, thereby covering more conduct than the proponent intended.

Mr. Fakhoury highlighted the fact that the privacy rights of the victim must be fairly weighed against the defendant's right to fully cross-examine and confront his or her accusers. And Mr. Fakhoury noted that the general identity theft statute is an applicable statutory remedy, so he questioned why we would need another law to handle this problem. Mr. Fakhoury also emphasized the potential issues of adding an abundance of new and different laws. New laws could be drafted sloppy or poorly and include ambiguous language that is left for courts to interpret, thereby covering more conduct than the proponent intended.
FTC SUES ALLEGED SNAKE OIL ENTERPRISE, ROCA LABS

By Hannah Yang
Business Editor

What would you do if you purchased something relatively expensive, were dissatisfied with it, could not return it, and could not share your product feedback or reviews with other customers? This is exactly the scenario that Roca Labs’ customers found themselves in, and the FTC is not happy. Roca Labs took their unfair and fraudulent claims and practices even further by attempting to censor any customer’s expression of dissatisfaction with their products, therefore creating a misleading and skewed body of testimonials and reviews.

Roca Labs’ weight loss formula claims to be an effective alternative to gastric bypass surgery. The company sells its products exclusively online, and targets its online advertisements at people who search for gastric bypass, or bariatric surgery, and other weight loss procedures. Considering the multi-faceted challenges of weight loss and general health and wellness, skepticism about Roca Labs products is plentiful. However, Roca Labs’ revenue is at least $20 million according to the FTC, which at the very least implies that there were buyers of the product.

Perhaps unsurprisingly, this case represents the first time the FTC has alleged that the use of these gag clauses is unfair, and thus a violation of Section 5 of the FTC Act. It is an error that we each hope will never result in major consequences, especially given the repeated advice that echoes in these halls: ‘Read before you sign’ or ‘If it’s too good to be true, then it probably is’ are widely known and widely espoused, but there are few among us who can say that they have taken the time to read the fine print. The knowledge that there are legal consequences upon the breach of a contract at least provides incentive to review a document before affixing a signature.

Unfortunately, the purchase agreement for Roca Labs’ “formula” included a “gag” or non-disparagement clause, a clause that prevents the customer from making any negative remarks about the company, product, or experience. According to the complaint, Roca Labs has allegedly threatened to sue individuals and used other intimidation tactics to enforce these gag clauses.

Consumer reviews, both positive and negative, are expected when a company puts product to market. It is a part of the process, where such feedback notifies the merchant of areas where improvement may be made to the product or service, and also informs other buyers. It is an important and necessary function of the market, and ultimately leads to advancements in technologies and new ideas.

The challenge of weight loss is physical, mental and emotional – and in this arena, there are no short cuts. Unfortunately, when a product is offered that purports to provide such a cut, the siren’s call is often irresistible to those who badly desire results. The FTC recognizing the troubling greed that operates in these spaces, works to curb the misleading and fraudulent business practices that lead consumers to fall victim to these schemes, demonstrated by the efforts undertaken here. A temporary restraining order has been granted against Roca Labs, with the hearing to show cause scheduled for later this month.

A MOTIVATOR AND REFRESHER: SERIAL PODCAST

By Kerry Duncan
Staff Writer

Almost a year ago, one of the most popular podcasts of all time was released: “Serial.” A spin-off of “This American Life,” the production focused on the murder of high school senior, Hae Min Lee, and the arrest of Adnan Syed, her former boyfriend. The podcast followed its creator, Sarah Koenig, as she investigated and searched for the boyfriend. The case, as well as another podcast, “Undisclosed,” provoked led to numerous legal blogs discussing the legal field took notice. The interest that was generated led to the legal community discussing what happened and even emotion is something that can help us in our profession to focus on legal questions that we must answer. On the other hand, the lay person that can be our clients and our witnesses in the future, focuses on the “facts.” This makes “Serial” a good reminder on how the general public can view a series of events versus how the general public sees it. Not only was the general public enthralled, the podcast followed its creator, Sarah Koenig, as she investigated and searched for the boyfriend. The case, as well as another podcast, “Undisclosed,” never hurts.

The fastest podcast to reach 5 million downloads in iTunes history, the series has a huge following that has fans independently investigating and sharing ideas all over the internet. “Serial” was awarded a Peabody for news, a first for a podcast, and an IDFA DocLab Award for Storytelling in 2014. Sarah Koenig was also named one of Time’s 100 Most Influential Pioneers for her work on the series.

An example of investigative journalism, Serial highlights some of the major differences between how law students can be trained to perceive situations versus how the general public sees it. Instead of accepting facts as they were given, each point was contested by the producers. This is something that can be absent in our casebooks. As law students, we do not usually fight the “hypo” or the facts. We more often focus on the questions of law. The removal of skepticism toward what happened and even emotion is something that can help us in our profession to focus on legal questions that we must answer. On the other hand, the lay person that can be our clients and our witnesses in the future, focuses on the “facts.” This makes “Serial” a good reminder on how the outside world can approach situations differently than a law student or lawyer might. It can also serve as a reminder to some of us why we wanted to be lawyers in the first place: to right a wrong, give closure to a family, defend the innocent. In the tangle of our textbooks and outlines, a reminder of the impact of what we do can be a blessing and motivator.

Not only was the general public enthralled, the legal field took notice. The interest that was provoked led to numerous legal blogs discussing the case, as well as another podcast, “Undisclosed: The State v. Adnan Syed.” Led by three lawyers, Rabia Chaudry, Colin Miller, and Susan Simpson, this podcast focuses instead on the legal arguments and defenses. It shines a different shade of light on the same case through the viewpoints of a family friend to the Syed family, an evidence professor, and a legal blogger for LL2. These viewpoints might be more familiar to our law school classrooms. The array of legal opinions on the same set of facts is a good reminder that there is not only one answer. Analysis remains king, a comforting thought as finals loom in the future.

At the end of it all, what we learn here in law school matters. Learning and seeing how the general public can view a series of events compared to how more legal focused minds can work, will only help us. Getting a helping hand of motivation from the importance of what we can do in the future through podcasts like “Serial” and “Undisclosed,” never hurts.
PETA GOES BANANAS, SUES ON BEHALF OF MONKEY THAT TOOK SELFIE

By Angela Habibi
Staff Writer

On September 22, 2015, People for the Ethical Treatment of Animals (“PETA”) filed a lawsuit against British nature photographer David Slater on behalf of a Sulawesi crested macaque monkey named Naruto. While Slater was on the Indonesian island of Sulawesi in 2011, Naruto swiped his camera and took a series of photos of himself. Slater used the San Francisco-based self-publishing company Blurb to publish a book called “Wildlife Personalities,” which included the ‘Monkey Selfies.’ As such, PETA claims Naruto owns a copyright in the now famous monkey selfies.

In order to represent Naruto, PETA is utilizing Federal Rule of Civil Procedure 17(c)(2), which reads in pertinent part that a minor who does not have a duly appointed representative may sue by a Next Friend. Further, according to the Complainant, PETA seeks a court order allowing all proceeds from the “sale, licensing, and other commercial uses of the Monkey Selfies...to be used solely for the benefit of Naruto, his family and his community, including the preservation of their habitat.”

In the U.S. a valid copyright requires an original work of authorship fixed in a tangible medium of expression. The Complaint here alleges that Naruto “authored the Monkey Selfies by his own independent, autonomous actions in examining and manipulating Slater’s unattended camera.” PETA attorney Jeffrey Kerr states that “copyright law is clear: it’s not the person who owns the camera, it’s the being who took the photograph” that should be granted the copyright. Thus, Kerr argues that Naruto owns the photos he took in the Indonesian jungle.

Can an animal be an author for the purposes of the U.S. Copyright Act?
The U.S. Copyright Office has been explicit in stating that animals may not be authors for the purposes of the Copyright Act and the Office’s Compendium states that it will not register works produced by “nature, animals, or plants.” To elaborate further, the Compendium states, “to qualify as a work of ‘authorship’ a work must be created by a human being [and] works that do not satisfy this requirement are not copyrightable.”

Kerr has said that the Copyright Office policy “is only an opinion [however] and that the U.S. Copyright Act itself does not contain language limiting copyrights to humans.” In fact, Kerr states that the “act grants copyright to authors of original works with no limit on species.” Because the plaintiff in this case is an animal and the Copyright Office is not a legislative body, or a court of law, having the question of whether a monkey may obtain a copyright before a judge raises interesting “administrative law questions, such as deference to the Copyright Office.”

While the claim of authorship by species other than homo sapiens may be novel, “authorship under the Copyright Act, 17 U.S.C. § 101 et seq., is sufficiently broad so as to permit the protections of the law to extend to any original work, including those created by Naruto.

Slater admitted in his book that “the recognition that animals have personality and should be granted rights to dignity and property would be a great thing.” Despite this however, he has countered PETA’s claims by stating that he was granted copyright protection for the photos in the U.K. and believes that the British copyright obtained by his company, Wildlife Personalities, Ltd. should be honored worldwide. Slater also argues that he was the intellect behind the photos because Naruto only pressed a button on a camera that Slater set up on his tripod.

Ultimately, although PETA’s cause is noble in seeking to assist animals that are critically endangered with proceeds from Naruto’s photographs, there is likely a better way to support the Sulawesi macaque population “than trying to set up a legal precedent where people have to try to get a monkey to sign a release form before they can post his selfie” anywhere.

U.S. AND CHINA INK ILLUSORY AGREEMENT ON CYBER ESPIONAGE

By Lisa Nordbakk
Staff Writer

“Protect your PC with virus protection.” “Antivirus Total Protection Instant Download.” “Get the best real-time security for your PC.” Do these compelling declarations sound familiar to you? Anti-virus and malware protection software providers such as McAfee, Bitdefender and Kaspersky are routinely offering their award-winning software to computer users. They promise to protect your passwords, e-mails, documents, and selfies from the modern-day burglars: the hackers. By simply following a few steps, they imply protection from criminals of cyberspace. This must mean that you are safe from treacherous Trojan horses, menacing malware, and vicious viruses, right?

Disappointingly, this is not the case. As the Imperva study revealed, the average detection rate of viruses lies at an abysmal 5%.

Most consumer anti-virus software can be downloaded for free, so at least corporations spending millions on cybersecurity are not as affected by this technological fragility, right? Cyber-defense teams working 24/7, with the support of first-rate corporate Anti-Virus Protection software such as Cisco, FireEye, and Palo Alto Networks must not be as penetrable by hackers, right? Wrong on both counts. Verizon’s 2013 Data Breach Investigations Report revealed that 62% of the intrusions against a business took at least two months to detect. A similar study conducted by Trustwave Holdings revealed that the average time of virus detection by top-trained corporate E-crime units was 210 days. So, best case scenario would give hackers two months to freely rummage through the corporate network; unfettered time to explore secrets, financial systems, and client data.

In the corporate world, the current cyber-combat places hackers on one side and corporate security teams on the other, the latter unfortunately being the losing side. Hackers have replaced rival companies’ approach of reverse-engineering technology and then replicating it with a shortcut: stealing blueprints, plans, and designs, and then simply duplicating the idea. The theft of American intellectual property is estimated to cause annual losses of $300 billion. Shockingly, the majority of this extortion can be attributed to one nation in particular: more than 50% of the losses of theft have the fingerprints of Chinese hackers on them. This equals the value of America’s total exports to Asia.

A Peace Treaty to End the Cyber War?
At the recent White House Summit, in response to this alarming trend, President Barack Obama and Chinese President Xi Jinping have reached a first of a kind cybersecurity agreement. At a joint press conference, Obama announced, “a common understanding” about the issue, and also alternatively took the opportunity to declare that the U.S. did not engage in cyber espionage. Xi named the agreement an “important consensus” on the issue of cyber crime, noting that “confrontation and fiction are not the right choice” for the two nations. The agreement pledges to have both sides investigate malicious cyber activity within their nations “in a manner consistent with their respective national laws and relevant international obligations.” Further, according to the fact sheet, the two leaders conceded to keep the victim nation updated “as appropriate” during such processes. To the extent of bi-annual meetings, where top-level officials in charge of the investigation will report on the progress, the victim country will not be involved in any of the investigations.

Truce or Empty Promise?
As promising and forward thinking as this agreement sounds, does it fall short of implementation, and therefore, just like malware protection software, does not offer a lasting solution to the issue of absolute cybersecurity? The fundamental problem of not having a functioning solution to tracking cyber attacks still prevails. Furthermore, it is left to the Chinese government to prosecute the perpetrators at their will. Therefore, the agreement, as idealistic as it sounds, does not guarantee any real investigation by Chinese authorities into the theft of IP or trade secrets. If there is no meaningful punishment, this agreement will likely fail to deter cyber criminals from continuing their illicit activities. Nevertheless, if the cyber attacks coming from China remain a threat to the U.S., there will be in a much better position to respond to these attacks and demand action from the Chinese authorities. Only time will tell if the Chinese government will put effective action where their rhetoric is.
A new form of fantasy sports is taking the country by storm. If you are a sports fan and are unfamiliar with the boom in Daily Fantasy Sports (DFS) by now, you are definitely in the minority. DFS are popular online games in which people can compete against others by earning points based on the actual statistical performance of professional athletes. In the past, the norm in fantasy sports was that contests would last entire seasons before a winner was declared, and contests typically only played for bragging rights among friends, and perhaps a marginal monetary prize. In stark contrast to this traditional practice of fantasy sports, DFS offers an accelerated version of fantasy sports where players can collect on a substantial amount of winnings in a single day against complete strangers. This recent surge in popularity of DFS is negatively impacting the average sports fan's experience watching the game.

Fanduel and DraftKings are the two companies that essentially dominate the unregulated multi-billion dollar industry. The reason for this is that these two websites are able to generate so much revenue because they take up to 10% of entered contestants wagers. Entry fees for contests range from $0.25 to $10,000, and the payout for these contests depend on the entry fee as well as the number of people in a given contest. If you have tuned in to ESPN, or watched any NFL game broadcast for that matter, it is almost certain that you have seen commercials enticing viewers to enter DFS contests. According to StatQviC, an analytics service that tracks television commercials, DFS offers have increased 30% since last season, and the average cost of a 30-second national airing is approximately $2,800,205. While the latest phones have the ability to be unlocked with a swipe of a finger, this technology is less secure if you have a biometric password. This is the reasoning behind the need for regulation in DFS. The SEC launched an investigation for insider trading on DFS. Public outrage claims that by having access to data and information other entrants did not have, DFS employees still only made approximately 0.3% of the $2 billion in winnings on the site, which would account for nearly $6 million of the websites’ total payouts.

The result of this report has certainly impacted the DFS industry as a whole. Leading sponsor ESPN has confirmed what DFS employees have suspected all along. While it will continue to allow advertisements on the channel, it will no longer include individual segments on DFS. DFS employees are not allowed to play DFS, and realized DFS employees make up approximately 9.3% of the $2 billion in winnings on the site, which would account for nearly $6 million of the websites’ total payouts.

The employees generally love it. While they are not allowed to participate in DFS leagues for monetary gain, it provides them with active exposure to fans outside their team’s market, as well as an opportunity to increase the value of their brand with additional cost to them.

DFS contests are certainly fun to play, but at what cost are they affecting the old-school fans that don’t participate in fantasy sports and simply want to watch for the love of the game? The DFS industry has come under fire in recent years for earnings that are ahead of the game. The DFS players love DFS, as do their team’s fans. With DFS, they can watch the emergence and the high popularity of daily fantasy sports as DFS offers an accelerated version of fantasy sports. While it remains to be true in the same level of skill as you, and not a shark who devotes his head-to-head matchup against one of your friends who is on the same team as you.

The SEC launched an investigation for insider trading and tried to obtain access to the data on his cell phone. Though defendant returned the phone to Capital One, the judge ruled he was not required to disclose the phone’s password. Although there is debate in the legal community as to whether DFS is a game or a contest, it is clear that DFS employees still only made approximately 0.3% of the $2 billion in winnings on the site, which would account for nearly $6 million of the websites’ total payouts.

The result of this report has certainly impacted the DFS industry as a whole. Leading sponsor ESPN has confirmed what DFS employees have suspected all along. While it will continue to allow advertisements on the channel, it will no longer include individual segments on DFS. DFS employees are not allowed to play DFS, and realized DFS employees make up approximately 9.3% of the $2 billion in winnings on the site, which would account for nearly $6 million of the websites’ total payouts.

The employees generally love it. While they are not allowed to participate in DFS leagues for monetary gain, it provides them with active exposure to fans outside their team’s market, as well as an opportunity to increase the value of their brand with additional cost to them.

DFS contests are certainly fun to play, but at what cost are they affecting the old-school fans that don’t participate in fantasy sports and simply want to watch for the love of the game? The DFS industry has come under fire in recent years for earnings that are ahead of the game. The DFS players love DFS, as do their team’s fans. With DFS, they can watch the emergence and the high popularity of daily fantasy sports as DFS offers an accelerated version of fantasy sports. While it remains to be true in the same level of skill as you, and not a shark who devotes his head-to-head matchup against one of your friends who is on the same team as you.

DFS employees were accused of taking advantage of inside information to win $350,000 off a single $25 entry in a contest on its rival site FanDuel. Public outrage claims that by having access to data and information other entrants did not have, DFS employees still only made approximately 0.3% of the $2 billion in winnings on the site, which would account for nearly $6 million of the websites’ total payouts.

The result of this report has certainly impacted the DFS industry as a whole. Leading sponsor ESPN has confirmed what DFS employees have suspected all along. While it will continue to allow advertisements on the channel, it will no longer include individual segments on DFS. DFS employees are not allowed to play DFS, and realized DFS employees make up approximately 9.3% of the $2 billion in winnings on the site, which would account for nearly $6 million of the websites’ total payouts.

The employees generally love it. While they are not allowed to participate in DFS leagues for monetary gain, it provides them with active exposure to fans outside their team’s market, as well as an opportunity to increase the value of their brand with additional cost to them.