SENATE JUDICIARY
EXHIBIT NO. 3
DATE 1/22/13
BILL NO. SB150

SB150 Testimony

From: Brendan O'Connor <ussjoin@ussjoin.com>
To: Robyn Driscoll
Subject: SB150 Testimony
Date: Jan 22, 2013 2:12 AM
Attachments: SB150Testimony.pdf

Senator Driscoll,

Please find attached my written testimony on SB 150, attached as a PDF. In addition, I have posted an electronic copy of my testimony to my blog, available at http://blog.ussjoin.com/2013/01/montana-drones.html . (The blog also contains a copy of the PDF, for ease of printing.) Please feel free to distribute this testimony, and that blog link, to anyone who has an interest in this material; in addition, I would encourage you to reiterate my offer to speak with any legislator via email or phone (the latter at 406-545-0430) about this important issue. (The offer is also present at the end of my written testimony.)

Thanks very much for your hard work on this issue.

Yours,

---Brendan O'Connor

Testimony on Montana Senate Bill 150, "An Act Limiting the Use of Unmanned Aerial Vehicles"*

Brendan O'Connor

January 22, 2013

Summary

- SB 150 protects the fundamental Constitutional rights of Montanans by preventing government agencies from using drones to surveil citizens, and by preventing drone-mounted weapons of any type from being used against Montanans.
- Current UAV technology allows every face to be seen and identified across more than 19 square miles, simultaneously, from an aircraft at 20,000 feet. This technology can be used to track every movement of every person even in Montana's largest cities.
- Law enforcement officials in other states have already deployed Taser-equipped UAVs; hobbyists have demonstrated that firearms can be mounted to drones as well, which would allow the "remote kill" functionality currently used in other countries to be used in Montana as well.
- SB 150 does not burden Montana's businesses in any way, allowing them to continue to grow the economy of the State of Montana with this new area of technology while also protecting Montana's citizens from governmental overreach.

My Background

My name is Brendan O'Connor. I am a fifth-generation Montanan; my mother grew up on her family's cattle ranch, halfway between Culbertson and Bainville; my great-great-grandfather was a homesteader, and I grew up in Billings. I am also a

*An electronic version of this document is available at `http://blog.ussjoin.com/2013/01/montana-drones.html`.

small-business owner; my company, Malice Afterthought,[1] is a Montana corporation which performs computer security research on behalf of businesses and the government. In 2012 alone, I presented on computer security issues at conferences in Washington, D.C., New York City, Las Vegas, and Dublin, Ireland. In the same year, my company won two separate research contracts from DARPA,[2] the long-range research group of the Department of Defense (whose work created both the Internet and, relevant to this testimony, the RQ-1 unmanned aerial vehicle, commonly known as the Predator drone[3]). I hold a security clearance from the Department of Defense, and I spent the first half of 2011 teaching at the military's cyberwarfare school. I hold both a Bachelor's and a Master's degree in Computer Science, with a research focus on computer security, from Johns Hopkins.[4] I am telling you these things because I want you to know that the issues surrounding unmanned aerial vehicles, especially as they impact the rights and freedoms of my fellow Montanans, are deeply important to me, and they have been of both personal and professional interest to me for years. You are welcome to consult my full resume, which is available on my website.[5]

This law, which Senator Driscoll is presenting to you today, was written while I was working for The Rutherford Institute,[6] an organization which is dedicated to the protection of civil liberties and human rights. The organization is often considered to be a leading conservative civil liberties group; indeed, in Montana, it partnered with my father, Bill O'Connor, successfully to protect the right of a student to thank God for her accomplishments as she graduated from high school in Butte, Montana.[7] I want you to know this because the issue of drones over Montana is not a partisan issue: I firmly believe that both Democrats and Republicans want the freedoms of the US and Montana Constitutions to continue to ring true for future generations.

Current Drone Capabilities

The abilities of current military UAVs[8] are relatively well-documented, if not generally directly experienced by the American public. Modern military UAVs view and record every action taken by every person in a full city simultaneously,[9] whether or not they are targets

[1] `http://www.maliceafterthought.com`

[2] The Defense Advanced Research Projects Agency; `http://www.darpa.mil/`.

[3] `http://en.wikipedia.org/wiki/General_Atomics_MQ-1_Predator`

[4] `http://cs.jhu.edu/`

[5] `http://ussjoin.com/resume.pdf`

[6] `https://www.rutherford.org/`

[7] "Court: Butte Graduation Speech Ban Unconstitutional," *The Billings Gazette*, `http://tinyurl.com/a4rx6lf`

[8] Unmanned Aerial Vehicle. Throughout this document, I will use the terms UAV and drone interchangeably.

[9] "With Air Force's Gorgon Drone 'we can see everything,'" *The Washington Post*, `http://tinyurl.com/2c638fy`

of interest at the time the recordings are taken, using technologies such as "Gorgon Stare" (capable of surveilling more than 19 square miles of land at a time, and identifying every face in that area simultaneously); analysts can then use "instant replay" technology (designed by the same people responsible for reality television camera operations) to access recordings from any time in the past, of and from any location in the field. UAVs that store video in these same systems range from tiny, hand-thrown drones with wingspans of just a few feet that can be carried in a backpack,[10] to the massive Avenger that stores its bombs and missiles inside its 16,000 pound hull.[11]

Of course, these are military drones, flying combat missions to protect our troops. Let us instead look at the UAVs flying over the United States. The Department of Homeland Security flies Predator drones (capable of carrying the same "Gorgon Stare" whole-city camera system as mentioned previously) from Corpus Christi, Texas,[12] and wants to purchase an additional 22 drones as soon as possible. **Many of these are intended to fly over Montana and other border states.**[13] For reference, only 61 of the current Predator model, the MQ-1C "Grey Eagle," have been produced for the whole world since 2004,[14] which means that the Department of Homeland Security wants to have the capacity to fight almost half as many full wars as the Department of Defense does, UAV-wise. **There is no difference in the technology being deployed between the military and DHS versions;** only the intent stated currently, at the outset, differs in any way.

This military technology is not confined to the Border Patrol; the Electronic Frontier Foundation compiled a list of the more than 700 authorizations to non-military entities (including universities, local police forces, and even sheriffs of rural counties) granted since 2004 (see Figure 1), and so now police forces can watch—and indeed, will be watching—every activity taking place over the area of an entire city, day or night, whether or not any wrongdoing takes place, and storing that data for future use. This technology is being employed so broadly that, as the EFF noted, **Otter Tail, Minnesota is planning to fly the same planes that were designed for combat zones.** Indeed, so many people are now needed to remotely control these UAVs that American aviation schools are now creating UAV "pilot" schools, and encouraging young people to "get a huge advantage" by studying this expanding field now.[15] While the FAA has not released information regarding any requests from Montana-based agencies to use drones, the EFF estimate that the FAA has yet to release information about fully half of the current licensees; current Montana law means that agencies are under no requirement to disclose these requests to the Legislature or any other body within the state. In addition, **Montana is currently surrounded by drone bases** (see Figure 2) whose UAVs will,

[10] "Raven RQ-11B Technical Specifications," `http://tinyurl.com/alf2rv9`

[11] "The Air Force Just Bought Its Biggest And Fastest Armed Drone Ever," *Business Insider*, `http://tinyurl.com/bh7n6or`

[12] "DHS starts Predator UAV flights in Texas," *Federal Computer Week*, `http://tinyurl.com/2dpfmgp`

[13] "DHS May Wait 14 Years To Complete Its UAV Fleet," *National Defense*, `http://tinyurl.com/2fve7z3`

[14] "MQ-1C Undergoing Development, Deployment," *Defense News*, `http://tinyurl.com/adr4ec3`

[15] "UAV Pilot License and Ratings," *Aviation Schools Online*, `http://tinyurl.com/bkn84qn`

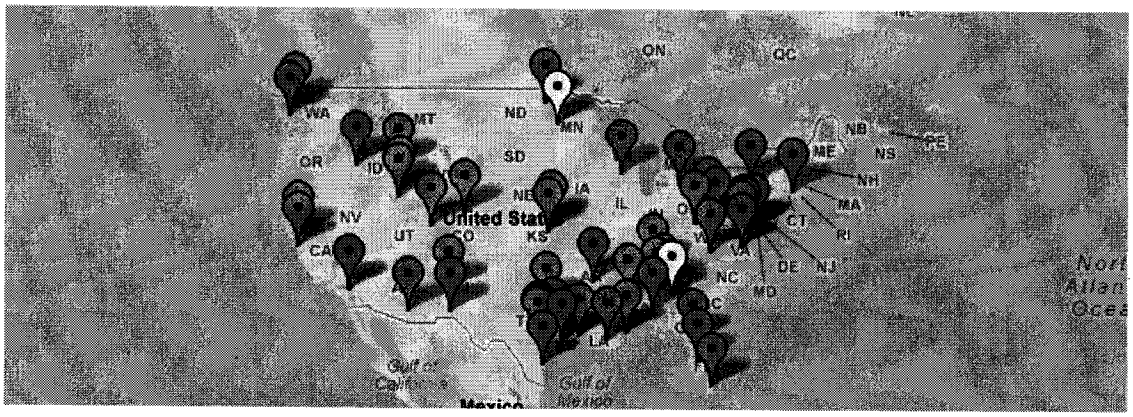

Figure 1: A map of UAV permits issued by the FAA to state and local agencies in the United States.[17]

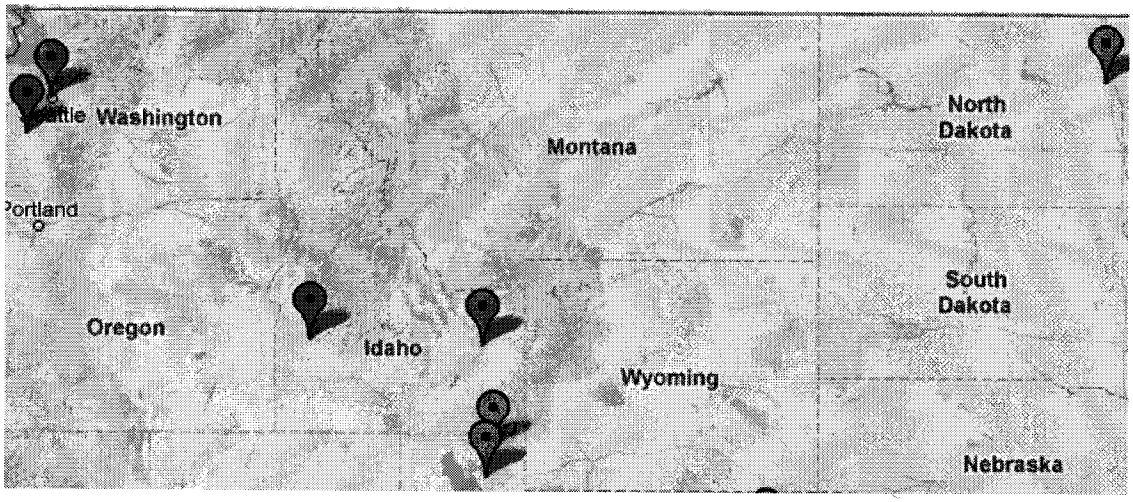

Figure 2: A map of UAV permits issued surrounding Montana.

just as with Air Force-owned drones (as noted below), "just happen" to overfly Montana. It is therefore a matter of certainty that Montanans are being captured by this technology every day, by an ever-increasing number of local, state, and federal agencies.

In addition to these civilian uses of drones, the Department of Defense operates 64 flight bases for UAVs in the United States.[18] Since these planes do, of course, have to traverse American airspace while flying to combat zones, their sensors will see the same range of legal human activity as any other drone in American airspace–and despite the "posse comitatus" rules prohibiting use of the military against American civilians without Congressional approval, the Air Force recently sent out a mandatory instruction instructing UAV teams to keep that footage for "up to" 90 days while it is examined for evidence of any possible wrongdoing.[19] Even assuming that it is not kept longer, it is an unprecedented

[17] Data courtesy of the Electronic Frontier Foundation. `http://tinyurl.com/cjb2ema`

[18] "Revealed: 64 Drone Bases on American Soil," *Wired*, `http://tinyurl.com/7ojeeez`

[19] "Oops! Air Force Drones Can Now (Accidentally) Spy on You," *Wired*, `http://tinyurl.com/blgtv9h`

step in the history of the use of military force against American citizens to allow them to keep a continuous log of all civilian activities for 90 days; since police can keep such footage permanently, however, one can imagine a *Truman Show*-style montage of every moment of one's life, captured for one's "convenience" from overhead. In addition to this "accidental" collection of footage, reporters have witnessed the Air Force intentionally instructing their unmanned drones to keep constant surveillance on private citizens' vehicles inside the United States, without a warrant, simply because they had nothing else to be doing.[20]

Emerging Drone Capabilities

UAVs are, at the moment, restricted by their size from some activities; it is hard to imagine a plane with a 30-foot wingspan peering into a home window. Science has, however, come to the UAV's rescue, and it has done so at an extremely attractive price point. For less than $1000, any person can own a powerful multicopter—a helicopter-type device with many separate propellers that allow it to hover in place for minutes or hours while capturing video, audio, and even thermal images. These devices can shoot incredible footage, and can be assembled using just basic tools from kits; some examples of their video quality and agility are demonstrated by the 2009 Mikrokopter project[21] and the 2012 QuadShot project.[22] Even toy manufacturers have gotten into the act; the Parrot AR.Drone 2.0, a $299 device sold on Amazon.com,[23] captures HD video in fantastic quality while streaming live to an iPhone, iPad, or Android device.[24] Even the previous version, which streamed only standard-definition video, is impressive enough; we took one outside at The Rutherford Institute to watch it in action, and were amazed by the capabilities of a device—controllable by children!—that contains technology reserved just a few years ago for the military. [25]

Meanwhile, science rushes onward, successfully mounting remote-control electronics on biological flying insects[26] and creating fully-artificial robots that look like natural hummingbirds in both size and appearance.[27] High-school students can now take parts from cheap robotics kits and use them to control the muscles on (real) cockroaches to steer them around a room.[28] Harvard University has even developed a bee-styled UAV that assembles like a pop-up book and has a body smaller than a penny. [29] With these new technologies, it will soon be essentially impossible to tell the difference between a normal

[20] "The Drone Zone", *New York Times*, `http://tinyurl.com/9wzm3m9`

[21] Video of the Mikrokopter is available at `http://youtu.be/-3U-n81RJtA`.

[22] Video of the QuadShot is available at `http://youtu.be/P6NDt1PCIDg?hd=1&t=2m30s`.

[23] `http://tinyurl.com/bbycpad`

[24] Video captured by the drone is available at `http://youtu.be/wpKRvHKW2U8?hd=1&t=34s`.

[25] `http://youtu.be/lCMjpsLVu7U`

[26] `http://youtu.be/PAeV96bTRiI`

[27] `http://youtu.be/7k_BzTu92Nc`

[28] `http://youtu.be/04T5Zq6KPyY`

[29] `http://youtu.be/VxSs1kGZQqc?hd=1&t=3m50s`

insect or animal and police surveillance without detailed inspection—and with pinhole cameras weighing nearly nothing, each of these devices can be used to capture every detail of someone's daily life. Indeed, one protective parent now uses a home-built UAV to walk his child to the bus each morning![30]

What This Law Would Do

SB 150 has two major purposes: one which creates a rule of criminal evidence, and one which creates a rule for the use of UAVs by government agencies in Montana (whether state or local).

Exclusionary Rule

The bill would create a blanket rule of evidence in criminal trials: UAV-collected evidence is inadmissible for any purpose. This means that courts and juries in Montana would not be able to hear drone evidence to determine the question of guilt or innocence; it also means that courts could not use drone evidence to determine the admissibility of *other* testimony into evidence.

The rule explicitly includes all UAV-collected evidence, regardless of its type (for instance, whether collected by listening to cellular phone calls, or by video recordings) or of who collected it. The latter is very important: since the federal government is not restricted by any state action in this area (due to the Supremacy Clause[31]), the state is unable to prevent the federal government from sending drones (owned by the military, the Department of Homeland Security, or any other organization) to surveil Montanans. What Montana *can* do, however, is restrict such evidence from being immediately turned over to and used by the state or local governments against their citizens. In a similar vein, this bill does not attempt to restrict private actors from using UAVs; for instance, a farmer might use a UAV to inspect his fields, or a real estate agent might use one to take pictures of a house for sale. If these drones happen to collect information outside their original mission, that information cannot be used as evidence; this prevents any effort to "get around" the law by simply contracting such work to a private entity.

[30] "Helicopter parent: Techy dad builds drone to hover over kid," *Christian Science Monitor*, `http://tinyurl.com/ceg2f5t`

[31] "This Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding." Constitution of the United States of America, Article VI.

Why A Warrant "Exception" Is Unacceptable

Clearly, UAVs can collect a large amount of data on law-abiding citizens without their knowledge or consent; in general, in the United States, we use warrants to restrict the police use of such surveillance technologies to situations where it can be shown that there is probable cause to believe that a crime has occurred. Why not use warrants to restrain UAVs?

Unfortunately, UAVs are different from normal surveillance technology, precisely due to their flight characteristics. As noted above, even the Air Force cannot control what their drones see en-route to an assigned mission; the same cameras that record a citizen's every waking action also keep the plane from, for instance, flying into a flock of geese. Requiring a warrant before recording citizens is simply unworkable; compliance with such a law would be impossible, and the requirement would therefore be meaningless.

In addition, the fact that unmanned aerial vehicles are, definitionally, unmanned, means that agencies can deploy near-limitless numbers of them to record, in essence, every waking (or sleeping) moment of every Montanan—regardless of whether any suspicion exists for any crime. This repository of all information will inexorably lead to abuse, whether it comes from people with access to the database (legal or otherwise) blackmailing citizens, or from agencies using facial recognition software to take down the names and personal information of anyone daring to show up to a political protest—or gun show. **Requiring agencies to commit personnel to tasks limits the potential for abuse.**

Even if the law did require a warrant to use a drone for surveillance, this is simply a minor procedural hurdle; regardless of merit, judges essentially never deny warrant requests, and magistrate judges charged with consideration of warrants often consider themselves to be an "extension of law enforcement."[32] Worse, even when warrants are not issued, the Supreme Court has ruled that as long as the police act in "good faith," the lack of a warrant is irrelevant.[33] Since as noted, drones cannot avoid collecting this data, "good faith" will prove to be universal. Warrants do not, therefore, stand as any realistic safeguard against the abuse of UAVs; thus **the addition of a warrant requirement for police use to this bill will destroy every safeguard the bill attempts to create, and destroy the Constitutional rights of the citizens of Montana.**

"Nothing to Hide"

A common refrain heard by opponents of surveillance is that if one has nothing to hide, one has nothing to fear from additional scrutiny. This is simply untrue; in addition to

[32] "Making *Leon* Worse," *Yale Law Journal*, `http://tinyurl.com/adz6x6u`

[33] *United States v. Leon*, 468 U.S. 897 (1984).

blackmail and extortion as noted above, citizens have a right not to have the most intimate moments of their lives surveilled by the government. Supreme Court Justice Brandeis remarked that the right of privacy was "the most comprehensive of rights, and the right most valued by a free people."[34] It is this right that was described most eloquently by Orwell in "1984," with the constant surveillance undertaken by "Big Brother" through the network of cameras in every citizen's home and throughout his or her life. That was not technologically possible when Orwell wrote his book; **unmanned aerial systems, by not requiring any human being to expend any effort whatsoever to record the innocent activities of a human, make Orwell's vision a reality.** It is imperative that the right of privacy be preserved not just in name, but in fact, by preventing the ceaseless recording of every private moment by flying robots—whether that private moment be a tender caress between husband and wife, a rancher tending his herd in the wee hours of the morning, or a hunter tracking an animal through the snow.

Anti-Personnel Capabilities

The bill also prohibits all governmental entities from using UAVs with anti-personnel devices, such as firearms, Taser-type electrical discharge weapons, or chemical agents such as "tear gas." Why is this important? While the military has, of course, armed drones for use outside our borders, this work has not been confined there; indeed, **the Department of Homeland Security purchased a Taser-equipped drone for the Montgomery County (Texas) Sheriff's Office in 2011.**[35] While that drone cost taxpayers $500,000 to purchase, these drones can be cheaply made; indeed, a hobbyist demonstrated that a handgun could be mounted to a drone costing less than $1,000 in total, with terrifying results caught on video.[36] Studies have shown that UAV operators are more likely to use deadly force in situations where it is not necessary, since they are not personally present at the scene and cannot see such nuances as unlikeliness to harm;[37] it is thus imperative that we protect the citizens of Montana from the accidental and unnecessary violence that is sure to result from these weapons being deployed as what could be seen as mere "crowd control" by a detached and impersonal user.

What SB 150 Will Not Do

It is also important to realize what SB 150 will not do. For one, it does not attempt to restrict the "airspace" of the State of Montana, as it has been repeatedly ruled by the

[34] *Olmstead v. U.S.*, 277 U.S. 438 (1928).

[35] "Taser Drone Launched in Texas," *Military.com*, `http://tinyurl.com/befpehj`

[36] "Man Arms DIY Drone With Paintball Handgun and Shoots Human Cardboard Cutouts," *BoingBoing*, `http://tinyurl.com/c8kn7pu`.

[37] " Air Force Drone Operators Report High Levels of Stress", *New York Times*, `http://tinyurl.com/au6zqur`.

courts that it is unconstitutional for a state to do so.[38] In addition, it does not restrict private entities, such as Montana's small businesses, from flying UAVs for private purposes (including real estate, farming and ranching, safety inspections, or a host of other positive purposes). There is no need to burden Montana businessmen and women with additional regulation, nor cut off any new business opportunities in which Montanans could take a leading role; without the criminal power of the state causing ubiquitous surveillance (and the chilling effects upon behavior it causes, as noted previously), natural business forces will allow Montana corporations to experiment with finding new ways to use UAVs for the betterment of all. Finally, it does not restrict citizens from using drone-collected data (such as the "accidentally"-collected footage discussed previously) in civil lawsuits; this means that, for instance, if a citizen is injured in an accident captured by a UAV, the data collected can be used to aid that citizen.

SB 150 thus represents an effective balance between the rights of the people to be free from unwarranted governmental interference, and the hopes and dreams of Montana's business community.

Conclusion

SB 150 defends the fundamental rights enshrined in the Montana and United States Constitutions from creeping technological overreach, on behalf of the citizens of the State of Montana. It is vitally important that this Legislature act to pass this bill, as it stands.

I am happy to answer any questions from any legislator about my testimony, about drone technology, or about the emerging capabilities of surveillance. Please feel welcome to contact me, either via email at `bfo@ussjoin.com`, or via phone at 406-545-0430. Thank you very much for your time and attention.

[38]See, for example, *City of Burbank v. Lockheed Air Terminal Inc.*, 411 U.S. 624 (1973); *Virginians for Dulles v. Volpe*, 541 F.2d 442 (4th Cir., 1976); *National Helicopter Corp. of America v. City of New York*, 137 F.3d 81 (2nd Cir., 1998); *U.S. v. City of New Haven*, 496 F.2d 452 (2nd Cir., 1974); *San Diego Unified Port Dist. v. Gianturco*, 651 F.2d 1306 (9th Cir., 1981).

Brendan Francis O'Connor

bfo@ussjoin.com

(406) 545-0430 http://ussjoin.com

Education

The University of Wisconsin - Madison *September 2011 - May 2014 (Ongoing)*
Juris Doctor

Dean's List, Spring 2012
Top 35% of class
Member, Pro Bono Society
Technology Administrator, Student Bar Association

The Johns Hopkins University *September 2006 - May 2009*
Master of Science in Engineering in Computer Science

Thesis Title: **Mnikr: Reputation Construction Through Human Trading of Distributed Social Identities**
President of the CS Honor Society, Upsilon Pi Epsilon

The Johns Hopkins University *September 2004 - May 2008*
Bachelor of Science in Computer Science

Graduated with Departmental Honors

Technical Experience

Malice Afterthought, Inc. *2010 - Present*
CTO / DSS

Malice Afterthought provides software and security consulting services to a range of clients, from small businesses to large corporations, in addition to creating and releasing its own commercial and open source software. From January - July 2011, I taught information and network warfare (CNO) to students of the Department of Defense. In January, 2012, we won a DARPA Cyber Fast Track research proposal to fund research entitled "Reticle: Leaderless Command and Control," and in November, an additional CFT proposal entitled "NOM: Novel Object Mapping." Please visit `http://www.maliceafterthought.com` for more information.

SET Corporation *2009 - 2010*
Senior Research Associate

I worked as a technical lead on software projects in a variety of areas, including natural language processing and user modeling, and a project to create an augmented reality application to add real-time data and intelligence analysis to a multi-viewpoint 3D holographic display using the iPhone 3GS. These software projects were for a variety of government agencies, including DARPA, AFRL, INSCOM, and the DoD.

Six Apart *2008 (Internship)*
Open Platforms Group

I worked as an engineer on the Open Platforms team, dealing with furthering the goals of data portability across technologies and corporate boundaries while maintaining a focus on user control of data. I worked as an intern full-time during the summer of 2008, and then part-time through the remainder of the year.

Sun Microsystems *2007 (Internship)*
Solaris Security Technologies Group

I ported and integrated software into Solaris allowing users to authenticate using true PKCS#11 interfaces, then worked with a variety of teams and people across Sun (despite my status as an intern) to move these smartcard services into Solaris. I also had the opportunity to work with DTrace on Solaris Kerberos.

VeriSign *2006 (Internship)*
Security Services

I worked primarily with the Unified Authentication group, specifically with One-Time Passwords; I also did some work for VeriSign Labs (the Advanced Projects Research Group) on the VeriSign Personal Identity Provider. Over the course of 12 weeks, I was responsible for major projects in C♯, Ruby, and Java, as well as JSP/Struts/Spring web applications, JNI, C/C++, and various technologies. Despite being an intern, I had the honor of winning the VeriSign Labs "PIP Challenge" for integrating one-time password technology with the VeriSign Personal Identity Provider.

Publications and Invited Lectures

Panel - The Global 'Gamification' of Online Gaming

Panel on the intersection between legal issues and cybersecurity research, especially as they affect the international online gambling industry. At the conference of the International Bar Association, Dublin, Ireland, on October 1, 2012.

Reticle: Dropping an Intelligent F-BOMB
Presented at the Security B-Sides (BSidesLV 2012) conference in Las Vegas, NV on July 26, 2012. Video and slides at `http://blog.ussjoin.com/2012/07/reticle.html` . The acceptance rate for talks was 53.75% (43/80).

Hack the Law
Presented at the Hackers on Planet Earth (HOPE Number Nine) conference in New York, NY on July 15, 2012. Video and slides at `http://blog.ussjoin.com/2012/07/hack-the-law.html` .

Sacrificial Computing for Land and Sky
Presented at the ShmooCon security conference in Washington, D.C. on January 27, 2012. The acceptance rate for talks at the conference was 16.6% (36/216). Average attendee review score: 4.52/5. Video and coverage (including Forbes, Wired, and MSNBC) collected at `http://tinyurl.com/84kmz8c`.

A "Fair and Balanced" Look at Online Privacy in the Age of Location-Based Social Networking
Presented to the students and faculty of the United World College of the American West in their symposium on social networking, April 9-11, 2010.

Mnikr: Reputation Construction Through Human Trading of Distributed Social Identities
O'Connor, B. F. and Griffin, J. L. Proceedings of the 5th ACM Workshop on Digital Identity Management. Presented at the ACM Computer and Communications Security conference in Chicago, IL, on November 13, 2009, and selected as the best paper at the workshop. The workshop acceptance rate was 33% (7/21) for full papers. `http://doi.acm.org/10.1145/1655028.1655032`

Federal Government and Major Organizational Endorsements

Department of Defense
Security Clearance (Contact for Details)

International Information Systems Security Certification Consortium, ISC^2
Certified Information Systems Security Professional (CISSP®)

Department of Homeland Security
IS-{100, 200, 700, 800, 802} - ARES/RACES Series
IS-{139, 230, 235, 240, 241, 242, 244} - FEMA Professional Development Series
IS-{1, 120, 130, 250, 288} - ARRL Advanced Emergency Communications Series
FEMA Professional Development Certificate

Federal Communications Commission
Amateur Extra Radio License, `K3QB`
Volunteer Examiner (Accredited through ARRL)

Amateur Radio Relay League
Public Service and Emergency Communications Management for Radio Amateurs (EC-016)
Amateur Radio Emergency Communications Course (ARECC)
Full Member, Dane County (Wisconsin) Amateur Radio Emergency Services

Legal Experience

Wisconsin Supreme Court *Fall 2012*
Judicial Intern
I served as a legal intern for Justice N. Patrick Crooks of the Wisconsin Supreme Court. My duties included examining cases requesting review by the Court, writing legal analyses of the issues raised by cases before the Court, and assisting the clerks in the performance of their duties.

The Rutherford Institute *Summer 2012*
Legal Intern
The Rutherford Institute is a public interest firm focusing on civil liberties litigation at both the trial and appellate levels, whose primary topics of interest are the First and Fourth Amendments as well as school "zero-tolerance" policies. I was responsible for legal research on current cases, drafting memos and briefs, and researching and writing legislation and policy statements for TRI on electronic privacy and UAV issues.