Feb. 14, 2013

Testimony HB 2093 / Proponent

Greeting Chairman Rubin and the House Correction and Juvenile Justice Committee. Thank you for this opportunity to provide support testimony for HB 2093, which would expand the crime of identity theft as it relates to computers or computer systems by adding social networking websites or personal electronic content to the current statues. The penalty in these cases for this bill would be a class A non person misdemeanor and according to the fiscal note it could potentially add two prison beds a year.

Today I bring this issue of Social Media identity theft to you because I believe that as a legislature we need to be looking at the growing trends of this powerful medium. Identity theft is nothing new, but now social media outlets, such as Facebook, Twitter, etc. are providing a new way for thieves to hijack identities. Within this new wave of technology and communication, social media affects all of our lives one way or another. Social and professional networking sites have millions of users. Facebook alone has over 4 million viewers per day, 1 billion active account users, 604 million mobile users, more than 42 million pages and 9 million apps actively utilizing social media to communicate.

No one ever expected such an explosion of social media in the 21st century. Social media communication is becoming more prevalent in the United States causing more states to take a closer look at their current policies, laws, and existing legislation regarding identity theft and online impersonation. According to Javelin Strategy and Research, about 12 million Americans got hit by identity fraud in 2011, a 13% increase from a year earlier, thanks to consumer's growing use of social-media websites and smart phones. And, 7% of Google+ users and 6.3% of those on Twitter reported a case of identity fraud.

According to the National Council of State Legislatures (NCSL), to date, 34 states have introduced or have pending legislation regarding identity theft or online impersonation during the 2012 legislative session:

- Alabama enacted three bills creating the Alabama Digital Crime Act, amending the definition of dealing in false identification documents and expanding the definition of identity theft to include using a person's identity to gain employment.
- California and New York both have new laws specifically banning online theft.
- Colorado added a surcharge for individuals convicted of identity theft against at-risk adults or juveniles.
- Kentucky and Michigan now allow exceptions to an insurer's use of credit information with regard to rates, rating classifications, tier placement and underwriting guidelines for specific life events, including identity theft.

- Louisiana and Mississippi created the crime of online impersonation and enacted the Business Identity Theft Prevention Act.
- North Carolina limited state agency identity theft reporting requirements.
- Utah lawmakers passed a bill requiring the Department of Workforces Services--if it learns during an eligibility check that a Social Security number is being used by an unauthorized person--to inform law enforcement and the Social Security number's owner.
- Virginia enacted legislation that requires local departments of social services to conduct annual credit checks on foster children 16 years and older to uncover and resolve cases of identity theft or misuse of personal identifying information.

Across the US and internationally there are many examples of social media identity theft cases that have actually happened. Here are a few examples for your consideration:

- **Johnston County, NC** – A Johnston County mother said she's been living a nightmare after her Facebook identity was stolen and used against her in a child custody dispute.
- **Washington County District Court** – A woman who thought she was connecting with a Facebook friend was actually manipulated by a Woodbury man determined to mine her personal data. Timothy Noirjean, 26, was accused of hacking women's Facebook accounts faced 13 counts of felony identity theft.
- **California** – a recent ruling define making false comments on someone else's Facboook as identity theft. Rolanda S, a juvenile resident, logged onto someone else's account, impersonated the rightful owner and made some public statements proclaiming a certain sexual fondness.
- **Northeastern England** - Julie Chambers lost her 2-year old daughter and discovered a fraudulent Facebook page with pictures of herself and her daughter, Zoe who died in 2008 after undergoing heart surgery. The site was taking donations for a transplant for Zoe, who was born with a heart valve that was too narrow. The Facebook page, traced back to Jamaica. The page also accepted donations to a personal PayPal account.
- **Bellville, New Jersey** – Dana Thornton, was charged with setting up a Facebook profile for her ex-boyfriend without his consent and using it to defame his reputation. She was indicted on one count of 4th degree identity theft. Allegedly, she created a Facebook page for former boyfriend and detective Michael Lasalandra after they broke up and posted pictures of him on it, posted disparaging and inflammatory comments defaming his character, lifestyle choices and career.
- **Judge Judy** – Terrorist Facebook Threats Nov. 9, 2012 and also aired this past Jan. 2013. A former best friend accused the other one of threatening her on Facebook. The friend was arrested and charged, but she denied the Facebook page and claimed it was a fake and not hers.

Although, the Internet knows no jurisdictional boundaries, it is imperative that we at least begin to protect the personal online privacy rights for citizens of Kansas by including HB2093's social media identity theft revision in the Kansas statutes. I ask that you favorably pass HB2093.

Respectfully Submitted,

Rep. Gail Finney
Kansas 84th District – Wichita; (316) 768-0615