April 22, 2016

Dear Vermont House Judiciary Committee:

Thank you for taking the time to hear my testimony. I am a computer scientist at Norwich University, where my research includes cryptography, computer security, and privacy. My testimony is my own, and I do not come here to represent my employer.

Before I start, I want to briefly discuss what privacy means, which is often swept under the rug in discussions like these. *"Only if you have something to hide should you be worried about privacy."* Some people believe incorrectly that privacy is about hiding a wrong: that is only a small part of the issue. Privacy is not just a form of secrecy—it's a collection of related issues that can result in harm if violated. It is, unfortunately, not as well understood or legally protected in the United States as it is in some other countries.

The most common argument you'll hear in favor of privacy goes something like this: Surveillance and security measures put in place by governments and the private sector can cause harmful **disclosure** of personal information. I argue that this is only one harm of many, including **aggregation**, **exclusion**, **secondary use**, and **distortion**.

**Aggregation** is harmful when pieces of information that are individually unremarkable or innocent are combined to be more revealing. For a trivial example, a purchase of a book about cancer alone is unlikely to be interesting by itself. Combine that with a purchase of a wig and suddenly medically-sensitive information like chemotherapy treatment can be inferred.

**Exclusion** is harmful when people do not have knowledge about how personal information about them is being used, and when they are unable to access the data or correct errors in the data. This causes a problematic imbalance of power between people and government (or between people and businesses).

**Secondary use** is the harm caused when data collected for one application is reused for a second, unrelated application without the person's permission. Considerations of data retention times and a user's rights to dictate how information about them is used are relevant here. For example, users of the genetic sequencing site 23AndMe and the genealogical site Ancestry.com have begun providing access to their DNA and familial databases to law enforcement in ways unanticipated by the user's original agreements. Related to this is a subtle increase in the scope of how data is used, such as in Vermont DMV's database of photographs, which is now used regularly by law enforcement.

**Distortion** is a harm that occurs when a person's personal information is used to create an inaccurate picture of a person. Since most data collected about a person is necessarily incomplete, it provides an incomplete picture of the person. Such data, spun the right way, can be used to mischaracterize and slander. The books that I read and websites I visit, for example, often cover the topic of hackers and criminal computer intrusion, including viruses and other malicious programs. It would not surprise me if I'd been put on a watchlist at some point for what I've read. That makes me a little sad.

Now that I've touched on what privacy is and why violating it can be more harmful than revelation of sensitive information, I'd like to briefly talk about privacy and security.

Security policies and expenditures are exercises in risk management—those incidents that

are predicted to be the most costly will get the most attention. There's never enough resources and we security professionals need to make decisions and conduct triage so our effort is spent most effectively.

Privacy breaches are something that economists refer to as externalities, where someone other than a decision maker pays the price for the results of a decision. When there's little overall cost to an organization in the event of a breach, there's little incentive for them to prevent a breach. In my roughly 15 years in the industry, I find that people are very often the weak link in security systems. Strengthening that link in the chain by enacting laws that have teeth and punish those responsible for disclosures is an important step. Such laws prevent breaches from becoming externalities, which at present, organizations feel safe to ignore.

A number of terrific items appear in S.155:

- Requiring a warrant for law enforcement access to communication services, including information like subject lines of emails or GPS locations is crucial. The language is also tailored to avoid bulk collection of data which can scoop up unrelated material.
- Providing the affected customer/subscriber with a copy of the warrant after the fact is important to the transparency of the system.
- Preventing drone use without a warrant, and explicitly preventing operators from connecting weapons and biometric recognition systems, is another positive step forward that balances law enforcement capabilities with residents' Fourth Amendment rights.
- Mandating that captured license plate data is not subject to subpoena and private litigation.

A number of items need some additional thought:

- Consider replacing the pop-cultural/colloquial word “drone” with the more descriptive “unmanned aerial vehicle”. Indeed, this term is used in the proposed language for 13 VSA § 4625(a)(4).
- Consider including IP addresses in the list of data that would require a warrant.
- Setting HIPAA as the standard for privacy of patient data sets the bar fairly low, and stands to benefit insurers more than customers, reinforcing the externalities of a breach.
- Medical records are a special type of data that do not change much over time. Once they're revealed, there's no way to put the genie back in the lamp. For this reason, we need to take the security of these records more seriously. The “Private Cause of Action” section struck by the Senate would allow individuals to pursue damages and injunctive relief would go a long way to dealing with the externalities of medical records. This is a pretty easy fix—very “low-hanging fruit” in my opinion. We should improve upon the protections of HIPAA and show people that their medical records are indeed secure.
- Including notifications of breaches would be an important step to strengthen the bill.

Thank you for the time you are spending on this important issue. This bill introduces a handful of incremental changes, but misses some big points. At some point, I hope that we will consider establishing a **fundamental** right to privacy such as is guaranteed in the laws of several countries. This is an idea that was first proposed in 1967 by privacy law pioneer Alan Westin in his book *Privacy and Freedom*. Please feel free to contact me with any questions you might have!

Sincerely,

Jeremy A. Hansen, PhD, CISSP
Assistant Professor of Computer Science, Norwich University
(802) 485-2221 (office) | (802) 279-6054 (mobile)| jhansen3@norwich.edu