The Electronic Privacy Act is a means to protect the 4th and 14th Amendment rights of Massachusetts citizens. This legislation will ensure that law enforcement agents are following fair procedure by requiring probable cause and obtaining a warrant to access the private electronic information of citizens.

Electronic Privacy

Add protection from unwarranted gathering of information from cell phones, laptops, and other electronic devices

■ The Bill

S.943: An Act to protect electronic privacy

■ Elevator Speech

We are Matthew Yan, Francesca Pinto, and Ashley Morales – and we are students of Brandeis University.

It is important that we, as American people, protect the freedom that our founding fathers fought for. As of right now, that freedom is at risk. Only through a simple extension of current electronic privacy law can we keep our personal information protected and maintain our constitutional freedom.

Based on the Electronic Communications Privacy Act passed in 1986, law enforcement can obtain electronic information without a warrant if it’s older than 180 days without informing you. This includes text messages, emails, records about your GPS location, and any other information that is stored online. These days, we carry almost all of our personal information at the convenience of our fingertips. This law is out of date and has left a gaping hole for law enforcement to manipulate. The fact that law enforcement can gain access to our personal information without a warrant if it’s older than 180 days is clearly a violation of our privacy.

The Electronic Privacy Act, H.2332, S.943, will close this gaping hole left by federal law by requiring law enforcement to get a warrant before obtaining personal information from a phone or internet company. Additionally, it will require a warrant in order to use an interception device known as a Stingray to trick your phone into giving out information. This piece of legislation will uphold our constitutional freedom through ensuring that law enforcement will follow fair procedure and obtain a warrant before receiving any private information. Will (insert name here) hold a hearing and vote the Electronic Privacy Act favorably out of the Joint Committee of the Judiciary?
The privacy of your electronic information is at risk. Under current law, law enforcement can obtain your personal information without a warrant if it’s older than 180 days. The Electronic Privacy Act will protect the information we carry in our phones and computers.

David Sabato, a physician, a husband, and a father, expresses his concerns with outdated digital privacy laws: “There is a huge risk without monitoring... the law should reflect justice based on technologies that are vital to living and surviving in this age”.

There is a bipartisan nationwide privacy push currently underway – various bills relating to electronic privacy are being introduced in 16 states, with bills already being passed in Virginia and West Virginia.

The Current Law is Outdated

The Electronic Communications and Privacy Act of 1986 was passed before the internet existed. This outdated act permits law enforcement to obtain electronic information without a warrant if it’s older than 180 days. Electronic info includes the contents of your emails and texts, your GPS location, and any information you store online. Current electronic law is simply out of date and has left a gaping hole in our protection of privacy.

Op-Ed

Francesca

Pushing for Privacy: Time to Update the Law

Photos of your graduation, text messages from your significant other, emails to your boss, Snapchat group messages with your best friends, private Instagram photos, Facebook messages, direct Twitter messages, your GPS location. You carry all of this information around with you every day on your cellphone. Only you have access to this personal electronic information. Well, maybe not.

That’s right. Based on the Electronic Communications Privacy Act passed in 1986, law enforcement can obtain your electronic information without a warrant if it’s older than six months. But wait a minute, wasn’t 1986 over 30 years ago? There have not been any amendments to the Electronic Communications Privacy Act in over 30 years. It’s not like there has been much technological innovation since then.

Police have a special device, called a Stingray, that they use to trick your phone into giving them information. Basically, what they do is they set up the Stingray in a certain location and the device gives them access to all the phones in a given radius. Let’s say that you are in a mall with a nearby Stingray. Without your knowledge, your phone is giving your personal electronic information to that Stingray device. Pretty intrusive, right? Well, there’s more.

Not only does the device acquire your data without your knowledge, but it holds onto all of that data. So even if police don’t need any of your data, the Stingray will keep it. This could have very well happened to you without your knowledge. Your text messages, your photos, and even emails that you drafted but never sent could all be stored on a Stingray device right now. Worried?

The Electronic Privacy Act, drafted by State Senator Karen Spilka, will require state law enforcement to obtain a warrant before acquiring any data from your phone or computer. In addition, it will require police to get a warrant before using a Stingray device. Once a Stingray is used, police will be required to erase all the data that the device collected that is not needed for an investigation.

Critics of the Electronic Privacy Act may claim that this bill will hinder police investigations by making them go through the extra step of getting a warrant. But what’s more important: completely violating our privacy rights to get the job done, or making police take an extra step to ensure our rights? This bill does not stop police from doing their job, it merely requires police to get a warrant before snooping into our lives.

Many people are unaware of the lack of electronic privacy and how law enforcement is taking advantage of obsolete federal laws. If your privacy is important to you and you feel uncomfortable with law enforcement accessing your personal electronic information without a warrant, call your local state legislators and tell them to support the Electronic Privacy Act, S.943, H.2332.
The current state of law as it relates to access to your digital information is based on the Electronic Communications Privacy Act passed in 1986, which is an outdated piece of legislation that no longer protects the privacy of citizens in this digital age. Current law allows for law enforcement to obtain electronic information without a warrant if it’s older than 180 days; including text messages, emails, records about your GPS location, and any other information that is stored online.

As technology is constantly developing and smartphone and cloud technology are becoming ever more present and necessary in day-to-day life, the legislation should be properly updated to reflect change in how digital information is housed as their own private spaces. This includes limiting the use of stingray technology, which tricks cell phones in the area into transmitting location and other identifying information that does not only gather the information of the targeted individual, but countless others who also happen to be nearby as innocent bystanders. That law enforcement is able to manipulate this gaping hole in current precedent without any need to notify that they would be doing so is a clear and overt violation of privacy.

The bill proposes that law enforcement obtain a warrant before demanding information – such as your emails, private social media messages and pictures, information you have on the cloud, and your contacts – from companies that store it. Massachusetts is not alone in the fight for privacy, 15 other states – in a bipartisan effort - are also fighting for legislation to maintain our freedoms, with bills having already been passed in Virginia and West Virginia.

Law enforcement may show some opposition to this bill, stating it would act as a potential barrier to their current procedure in acquiring information. However, the bill simply provides a fair system that protects the constitutional rights of citizens. It merely updates legislation with a more contemporary view on the privacy and acquisition of information at no additional financial cost to the Commonwealth.

Representative Dempsey, this bill is a proponent of progress and protection of our rights and freedoms. We ask that when the Electronic Privacy Act comes to the Ways and Means Committee you will vote favorably on it as a no-cost update to outdated legislation.

**Letter to the Legislator**

As citizens of this country, we believe that protecting our personal information is an essential component to our freedom. We are reaching out to you because our freedom is at risk. Did you know that under current law, police can look through your saved emails, text messages, and other electronic information after six months without a warrant? As young leaders of this generation, we need your help to protect our freedom, including your own. We are certain that someone such as yourself has a lot of important electronic information stored on your cellphone. How would it make you feel to know that law enforcement has the ability to access that private information without a warrant? Emails to your colleagues, text messages to your family, photographs, and information about your location all have the potential to be accessed without your permission.

The Electronic Privacy Act (S.943) closes a gaping hole left by an obsolete federal law that says law enforcement can obtain your information without a warrant if it’s older than 180 days. Under federal law, the government can claim authority to read all your old correspondence, and even emails you drafted but decided to NOT send.

The new bill would merely require law enforcement to obtain a warrant before demanding information such as search queries, emails, chats and texts, private social media messages, and other electronic information. In addition, there would be no financial implications as the bill would act as an update to current legislation to reflect our privacy rights as they regard the current state of technology and digital information.

It is imperative that we update the law to reflect the way we use technology today. The Electronic Privacy Act will implement a fair procedure for police to follow while maintaining our constitutional rights.

As of now, the Electronic Privacy Act is in the Joint Committee on the Judiciary. Will you speak in support of the Electronic Privacy Act with your colleagues who sit on the Committee on the Judiciary in order to help the bill get voted out favorably?

**Excerpts from Campaign Journals**

**Ashley**

*Meeting with Representative John J. Mahoney's office*

I thought this meeting was very important because I really found the meetings where I could inform people about the bill and teach them something they didn’t really know. I remember this meeting was the first time that we were asked a question that we couldn’t answer and had been asking ourselves a lot through the process of investigating our bill—how much are the police really using stingrays and searching through citizens’ data?

It was a big milestone in having to admit that we didn't know, but also that it wasn't really possible to check because the police don't really report this information. This question also helped illustrate to me what people who don't know the bill really are interested in knowing when deciding if the Electronic Privacy Act is of importance to them or not; based
on how much they think their privacy is being abused, they see why we need this bill to pass. I left this meeting thinking about how to address this point in our legislative report and upcoming advocacy projects in order to stress why the Electronic Privacy Act is important.

Francesca
Matt and I went to the State House and met with Aaron Carty, who is an associate counsel for the Senate Committee on Ways and Means. He works for Senator Karen Spilka, who is presenting the Electronic Privacy Act, and helped to draft the bill. He was an extremely helpful person to meet with because he clarified a lot of information and language in the bill that was difficult for me to understand. Additionally, he went through the entire legislative process with us which helped me to better understand where the bill was at that point in time and what exactly needed to happen in order for the bill to pass.

Not only did Aaron clarify the bill and current problems with privacy laws, but one extremely useful tool he provided us with was who we needed to speak with to start bringing awareness to privacy issues and help get this bill passed. Aaron explained that this bill had been passed multiple times through the Senate, but not through the House. He suggested that we meet with as many House members as we could and explain the bill since many people don’t know that much about it, especially the way police utilize Stingray technology.

Something else I took away from our meeting with Aaron is the importance of following up and maintaining relationships with who you meet. Since our meeting with Aaron, I have kept in contact with him through email. There have been multiple times over the course of the past few months that I have had specific questions about the Electronic Privacy Act which Aaron has been able to help me with. I think that following up and maintaining relationships with who you meet is vital, especially in the legislative process.

Matt
The Electronic Privacy Act is, for the most part, an issue of an uninformed public. By no fault of their own, they are unaware of law enforcement tools (stingrays) used to invade privacy because law enforcement worked to make sure that it remained unknown. We asked Ms. Hearn and Mr. Barash about how much they knew about the issue, and they both had vague, cursory knowledge – both knew that law enforcement might have the ability to track phones, but know less about the specifics of stingray technology. We introduced the issue as one where current legal precedent needs to be updated, explained what information stingrays are able to see/take, and ended with the demands of the bill (requiring a warrant before stingray usage so that the 180-day rule would no longer be in effect).

They both asked us quick questions about the context for the bill, to which we typically brought up the state of technology in 1986, when the original piece of legislation was passed that has near to no relevance to our current tech usage, and simple terminology like IMSI (International Mobile Subscriber Identity) to explain the scale of privacy invasion. We were also asked about immediate effects: ex. “If police set a stingray outside the statehouse, they would be able to access all of our information right now.” To which we answered “Yes.”

I do not think we made very deep connections with these legislators, but I think we achieved our goal of informing them of the issues that hopefully they will keep in mind further down the line.

Update
The bill was scheduled for a hearing on June 5, 2017.

For more information
View the Bill:
malegislature.gov/Bills/190/S943

American Civil Liberties Union:
aclu.org/issues/privacy-technology