Debate Essay: Law Enforcement Need for Backdoors into Devices and Software

Laura L. Lamoureux

IST 618

Syracuse University

**Debate Motion**

Security - Criminals use the advances in information technologies to perpetuate and further their criminal activity in ways that can go undetected. DHS, FBI and other law enforcement entities are facing significant challenges in combating crime in cyberspace. Whether it is domestic or foreign terrorism, disinformation campaigns, hacks, surveillance or other issues, there are unique implications on security in the digital age and governments should have as many tools in their toolkit they need. Apple and other cellular companies must create a backdoor for law enforcement to defend national security.

**Opening Statement**

Law enforcement needs all possible tools in its toolbelt in order to prevent, stop and solve crimes. One missing tool in today’s world, is the ability to get into encrypted devices, i.e. a backdoor. It isn’t just about getting into a device; it’s also about getting into a device in a timely manner. If lives are at stake as they often can be in a terrorist attack; we do not need to be hampering law enforcements efforts to protect our citizens. If people are innocent, then they have nothing to fear with law enforcement having this tool available to them.

**Presentation of Argument 1: Needed for National Security**

In 2015 a private data security firm conducted a market survey around the topic of backdoor governmental access. “The survey found that 63% of respondents supported backdoor access by government entities even when knowing the risks”. (Forbes, 2015). That’s a pretty high number of Americans that think it’s a good idea to grant the government access – even at the expense of their privacy. Of course, this is all in the name of national security. The survey results also showed that “58% of respondents believe that terrorist threats will be easier stop; and 41% percent thought major domestic criminal activity would be more easily halted”. Now the particular parameters of this survey aren’t readily available; however, it is telling that when the argument is framed as “needed for national security” Americans want government entities to have the access that they need to.

James Comey, former Director of the FBI has said, “Today, there are countless providers, countless networks, and countless means of communicating.” (Comey, 2014) Law enforcement needs to be on the forefront of keeping us safe. In order to do that they must have a greater capability for thwarting evil wherever it may lie. The one missing capability is to gather information from an individual through the resources they themselves are using: chat messaging, hidden software, etc.

Law enforcement lags behind criminals in its ability to be able to switch technologies on the fly. Bad actors can move from cell service to wi-fi; from one app to another app without a step in between. Law enforcement is hindered by that type of movability. There’s no real opportunity for them to get in front of action; to be able to offer prevention as well as stopping an activity. Innocent people have nothing to worry about.

**Presentation of Argument 2: Business vs Consumers**

Businesses vs consumers. “Encryption can protect either businesses or consumers from cybercriminals.” (Martin, 2019) But not both. Our economy is built on the notion that business will do what they must (and they must) to protect their data and their customers/clients/consumers data (this includes business information as well as employee information). Some businesses are even held to a stricter standard by law. And almost all businesses run the risk of being held liable if their data and their consumers data is compromised. We see this all the time with data breaches. Most businesses use some sort of enterprise encryption software that allows them to protect their information. What’s critical here, is that all enterprise encryption software have key recovery systems in place in case someone at the business loses or forgets the key. This is a backdoor…in place … already.

Individuals on the other hand are often (notoriously so) unconcerned when it comes to their own habits safeguarding their information. Password notebooks carried in purses, password notes saved on an unlocked phone, a company password taped to the underside of the keyboard (‘cause no one ever looks there!) just to name a few examples of our habits. If it wasn’t for business like Apple and Google putting those safeguards in place for the end-user, most end-users would not bother. Therefore, having backdoors in for law enforcement has the potential to save us all.

**Presentation of Argument 3: With Social Media Usage, Nothing is Private**

“Information is collected on social media sites in ways that might not be obvious to social media users.” (Lindsey, 2019) In today’s world, a social media presence is everything, from businesses and celebrities, to adolescents and grandparents. Some businesses even skip a regular website and just operate from Facebook or Instagram. Identities are built and torn down based on social media praise and condemnation. There is so much power in a social media presence. People share their love and hate for each other, for products, for experiences; they share their lives.

We’ve all heard/read/seen on social media stories about people documenting their vacations; and criminals using the social media information to find out where they live and break in to their homes. Stories about people being bullied in cyberspace and stalked in real based on their social media presence. So it leads to the question… if you are already sharing everything… why do you care about your digital privacy from law enforcement?

You have already broken that privacy wall, so to speak, if you have already shared your information (it’s all information) on social media. You may think it’s only shared with people “I know”. But what about people they know; and then people that know those secondary people? All of this implies, a lack of true concern about privacy. If that is the case, there should be little concern for law enforcement for wanting a backdoor into encryption and/or devices to prevent and stop crime. Law Enforcement is already using social media to find criminals.

**Closing Statement**

One of the main tenants of government is to protect its people. In order for the government to do that, it must have all the tools in that toolbelt. That includes the use of a backdoor. It seems odd that we’ve turned our lives over for their protection, yet we attempt to prevent them from doing so. Is it so impossible that this can’t be made possible? Let’s help Law Enforcement do what we’ve asked them to do. There is already encryption backdoors with key recovery systems in place, there is a significant lack of privacy accepted with social media practices and our national need for security is critical in the perilous times we live in. Let them in, it’s the best thing we can do for law enforcement and our safety.

**Questions for the Opposition**

1. How are privacy concerns for one individual more important than health and safety concerns of our nation’s citizens?
2. With all the technology “smartness” in the world, why isn’t it possible for a law enforcement backdoor that would not weaken the entire system?
3. What about your social media habits? What is your privacy expectation as it relates to your social media presence?

**Arguments the Opposition is Going to Pose**

1. What about individual privacy concerns? This is about individuals concerns. It is about protecting them from imminent danger. The longer it takes Law Enforcement to break into (brute force) a device or software, the more many, many citizens are placed in harm’s way.
2. Having a backdoor in place, makes an cyberattack easier for bad actors, how does this make us safer? It is a balancing of priorities. Preventing and stopping crimes is a critical focus of law enforcement work, a backdoor is necessary for that work to be at top level. Also, with law enforcement presence with the backdoor, cybercrime could potentially be prevented before it happens or at the very least, stopped before too much damage is inflicted.

Excluding title page and references, word count for this document is 1241.

**References**

Martin, L. (2019). Why Encryption Backdoors are No Worries for the Enterprise. *TechBeacon*. Retrieved from: <https://techbeacon.com/security/why-encryption-backdoors-are-no-worries-enterprise>

Grauer, Y. (2015, September). Most Americans Support Government Backdoors, Even Though They Know the Risks. *Forbes*. Retrieved from: <https://www.forbes.com/sites/ygrauer/2015/09/11/government-backdoors/#697846b3472e>

Johnson, A. (2020, March). A Backdoor Attempt to Require Backdoors to Encryption. *Morning Consult*. Retrieved from: <https://morningconsult.com/opinions/a-backdoor-attempt-to-require-backdoors-to-encryption/>

Comey, J. (2014, October). Going Dark: Are Technology, Privacy and Public Safety on a Collision Course? *FBI Speeches*. Retrieved from: <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>

Madden, M. (2012, February). Privacy Management on Social Media Sites. *Pew Internet & American Life Project*. Retrieved from: <https://beta.images.theglobeandmail.com/archive/01377/Privacy_management_1377894a.pdf>

Lindsey, N. (2019, February). New Research Shows that Social Media Privacy Might Not Be Possible. *CPO Magazine*. Retrieved from: <https://www.cpomagazine.com/data-privacy/new-research-study-shows-that-social-media-privacy-might-not-be-possible/>

Choi, Y.H. (2014, December). Self-Disclosure Characteristics and Motivations in Social Media: Extending the Functional Model to Multiple Social Network Sites. *Human Communication Research*. Retrieved from: [https://onlinelibrary-wiley-com.libezproxy2.syr.edu/‌doi/full/‌10.1111/‌hcre.12053](https://onlinelibrary-wiley-com.libezproxy2.syr.edu/doi/full/10.1111/hcre.12053)