INTERHACK

Interhack
5 E Long St 9th Fl
Columbus, OH 43215

VOX +1 614 545 HACK
FAX +1 614 545 0076
WEB http://web.interhack.com/

Risks Presented by Foreign-Controlled Software

C. Matthew Curtin, CISSP

May 17, 2023

We manage information through computer systems. Anyone who controls computer systems has the ability to make them behave in ways contrary to the requirements and expectations of their users. Systems under the control of foreign actors present risks to their users, people whose information is managed by them, and the institutions that rely upon them.

In today's remarks, I summarize several points for consideration as the Technology and Innovation Committee considers House Bill 17. First I present my background for offering these conclusions.

Background

I am a computer scientist and the Founder of Interhack Corporation, based in Columbus. My professional practice focuses on the science and technology of computing and information management, with applications including privacy, security, and forensics. I spent sixteen years as a part-time faculty member at the Department of Computer Science and Engineering at The Ohio State University and have authored numerous papers and books on privacy and security.

Detailed Information Collection

Computer systems today include everything from the large systems few people ever see to mobile devices including phones, tablets, and even wearable devices. Networking the devices together allows for a global system of information and computing.

As information is stored electronically, we don't access the physical media as we did with paper. In fact, we depend entirely upon software and the hardware of computing to capture, transmit, store, and present information. If we cannot trust that computing infrastructure, we cannot trust the information.

The phones that almost all of us carry include the ability to capture, store, and transmit information.

1. Location can be determined through several methods, including Global Positioning System (GPS)[1] signals, as well as analysis of signals in the mobile networks that support them.[2]
2. Text, audio, photo, and video data presented to the user must be on the device. Displays can be captured—either as a "screenshot" or a video of screen activity.
3. Microphones present on such devices can capture audio. Not only are the microphones available for use for telephone calls but are available to apps that run on these devices. Voice-activated services require that these microphones are always on, such that the audio cue to take action can be received.
4. Cameras present on such devices can capture photos and videos, often from either side of the device. Data formats for photos allow for augmentation to include, for example, location data.[3]

[1] See, generally, https://www.gps.gov/.

[2] José A. del Peral-Rosado, Ronald Raulefs, José A. López-Salcedo, and Gonzalo Seco-Granados. Survey of cellular mobile radio localization methods: From 1g to 5g. *IEEE Communications Surveys & Tutorials*, 20(2):1124–1148, 2018. DOI: 10.1109/COMST.2017.2785181

[3] Paul Alvarez. Using extended file information (exif) file headers in digital evidence analysis. *International Journal of Digital Evidence*, 2(3):1–5, 2004

In my experience, I have found that many people simply give no thought to how these systems are connected. As an example, when I spoke at the National Association of Criminal Defense Lawyers' Fourth Amendment Seminar, I asked how many attorneys use an Amazon Alexa in their offices. Many hands went up. I asked a slightly different way: how many attorneys have a voice-activated device in their offices. Again I asked a different way: how many attorneys have an always-on microphone in their offices. Finally: how many attorneys have an always-on microphone controlled by a third party in their offices where they have privileged conversations with their clients and cocounsel.

Security and Privacy Risks Well Documented

Security and privacy risks are not new. My firm's own Internet Privacy Project documented several cases where systems collected information about people and their interactions on web sites. Our work at the beginning of this century showed how tracking of activity was often surreptitious and performed by third parties, allowing them to develop detailed dossiers.[4] Concerns over these issues has led to a body of litigation on the matter of privacy policies, generally requiring—at least theoretically, notice to users and their consent.

Despite the presence of policies, systems have in many cases found to behave contrary to their policies, and even contrary to law. After European policymakers adopted privacy law, Google was fined for violating the law.[5]

[4] Matt Curtin. *Developing Trust: Online Privacy and Security*. Apress, November 2001

[5] Adam Satariano. Google is fined $57 million under europe's data privacy law. New York Times, January 2019. URL https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html

Impact on Private Information

"If you are not paying for the product, you are the product" is a common but oft-unheeded warning. Detailed information collection and aggregation continues, often built into a model of supporting access to goods or services without requiring direct payment by the consumer.

In addition, information is often stored "in the cloud," as what is captured requires storage capability far beyond what mobile devices can maintain. People often also want to be able to get to their photos, videos, email, and other information from any device. Cloud providers have been the subject of subpœnas to produce the information in litigation and in criminal investigations.

Organizations have also been the subject of *denial-of-service* attacks, where someone is able to shut down critical computer systems that can bring organizations to a halt. In some cases, these are simple acts of revenge (*e.g.*, a disgruntled ex-employee),[6] or in others they are attempts to extort payment to restore service.

Increasingly, large data stores are the target of a different type of ransom attacks, where information is accessed and extracted. The attacker then extorts the information holder: make a payment or have the information published or sold.

The notion of "private information" becomes dependent on a large number of conditions outside of the understanding, much less control, of individual consumers.

Allegations of corporate espionage of American companies are also well-documented.[7] Assessing likely motivations for corporate espionage might seem straightforward. (Why invest in research and development when you can steal the results?) Implications for Government might prove more difficult.

[6] United States Attorney's Office Northern District of Georgia. IT manager sentenced for hacking into and sabotaging his former employerâĂŹs computer network. Press Release, May 2020. URL https://www.justice.gov/usao-ndga/pr/it-manager-sentenced-hacking-and-sabotaging-his-former-employer-

[7] Ana Swanson. *U.S. Tech Espionage Team Unveils First Cases Involving China and Russia*, May 2023. URL https://www.nytimes.com/2023/05/16/us/politics/sanctions-tech-espionage-china-russia.html

Implications of Access to Private Information

As I understand House Bill 17 it specifically addresses this threat against one threat actor, the People's Republic of China. The Center for Strategic & International Studies has reported how the Chinese Communist Party has been working to increase its authority within Chinese companies.[8] Many expect that this means Chines companies must increasingly do the Party's bidding.

Trust in Government institutions can be undermined through loss of confidence in their ability to protect information. Private information must have confidentiality. Even public records have security concerns: they must have integrity. Imagine the consequences of the ability to make changes to records.

[8] Scott Livingston. The new challenge of communist corporate governance. CSIS Brief, January 2021. URL https://www.csis.org/analysis/new-challenge-communist-corporate-governance

Implications of Access to Systems

The literature of computer science shows a longstanding effort to implement *trusted computing*, generally, a foundation that we can reasonably rely on to ensure that it is under our control.[9] Systems exist to provide these features to varying degrees, but they are not common in daily office use. In any case, where users have the ability to install or to use software that cannot be trusted—whether because of error, omission, or hostile intent—a risk to such systems and the institutions that use them exists.

Considering the threat posed to an organization, including a state or local government by weaponization of software[10] is reasonable. Widely-deployed software has the ability to introduce massive disruption to critical systems through overload, exposure of sensitive information, and more.

No system or organization can be completely secure against all threats. Nevertheless reasonably foreseeable attacks can be addressed, and steps can be taken to ensure affirmative control over critical information infrastructure. Limitation of software based on both business case and origin of systems can be one effective measure.

[9] Andrew Martin. The ten-page introduction to trusted computing. 2008

[10] Kevin W. Hamlen. Stealthy software: Next-generation cyber-attacks and defenses. In *2013 IEEE International Conference on Intelligence and Security Informatics*, pages 109–112, 2013. DOI: 10.1109/ISI.2013.6578797

Bibliography

Paul Alvarez. Using extended file information (exif) file headers in digital evidence analysis. *International Journal of Digital Evidence*, 2(3):1–5, 2004.

Matt Curtin. *Developing Trust: Online Privacy and Security*. Apress, November 2001.

José A. del Peral-Rosado, Ronald Raulefs, José A. López-Salcedo, and Gonzalo Seco-Granados. Survey of cellular mobile radio localization methods: From 1g to 5g. *IEEE Communications Surveys & Tutorials*, 20(2):1124–1148, 2018. DOI: 10.1109/COMST.2017.2785181.

Kevin W. Hamlen. Stealthy software: Next-generation cyber-attacks and defenses. In *2013 IEEE International Conference on Intelligence and Security Informatics*, pages 109–112, 2013. DOI: 10.1109/ISI.2013.6578797.

Scott Livingston. The new challenge of communist corporate governance. CSIS Brief, January 2021. URL https://www.csis.org/analysis/new-challenge-communist-corporate-governance.

Andrew Martin. The ten-page introduction to trusted computing. 2008.

Adam Satariano. Google is fined $57 million under europe's data privacy law. New York Times, January 2019. URL https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html.

Ana Swanson. *U.S. Tech Espionage Team Unveils First Cases Involving China and Russia*, May 2023. URL https://www.nytimes.com/2023/05/16/us/politics/sanctions-tech-espionage-china-russia.html.

United States Attorney's Office Northern District of Georgia. IT manager sentenced for hacking into and sabotaging his former employerâĂŹs computer network. Press Release, May 2020. URL https://www.justice.gov/usao-ndga/pr/it-manager-sentenced-hacking-and-sabotaging-his-former-employer-s-computer-network.