

Statement Submitted to the Standing Senate Committee on National Security, Defence and Veterans Affairs, Senate of Canada

Explaining Concerns About Bill C-22 Based on Experience with Prior Encryption Proposals and Lawful Access Regimes Elsewhere

Ian Goldberg, Michael Specter, Douglas Stebila, Peter Swire

Law enforcement and intelligence services in Canada have supported Bill C-22 as a way to require technical assistance from electronic service providers in bypassing the encryption used to protect private messages and emails. This document draws on the authors' years of experience analyzing prior proposals related to encryption and lawful government access to evidence. **Despite the commendable goals of Bill C-22, to enhance public safety, the bill as written has serious flaws that amendments can and should fix.**

Our discussion focuses on the version of C-22 that was revised in June 2026 and passed by the House of Commons. **Law enforcement officials have argued that new tools to access encrypted data are necessary to solve serious crimes.** For instance, in August, as reported in the Edmonton Journal, Ontario Provincial Police Commissioner Tom Carrique [said](#): "Under a search warrant, we need the ability to get to that encrypted data or we can't solve homicides. We can't protect children from sexual exploitation. We cannot disrupt terrorist cells." He added, "I think Canadians need to ask themselves, is it acceptable that criminal organizations, drug cartels that are orchestrating homicides in this country are using encrypted technology to orchestrate those hits."

Having worked for years on cryptography and related policy issues, we know that **decades of cryptographic research and expertise**, including the widely cited ["Keys Under Doormats" report](#), **demonstrate that any mechanism letting a third party access properly encrypted content necessarily weakens security against all other attackers**, including hostile intelligence services and organized crime. The bill hopes that it can define this away by focusing on individuals targeted with a warrant, but exceptional access cannot be engineered to work only against specific users: a key or backdoor that works for one individual can, once built, be stolen or misused against everyone.

In assessing the most recent version of C-22, we bring longstanding experience in technical, legal, and policy aspects of encryption. Ian Goldberg is the Canada Research Chair in Privacy Enhancing Technologies, and a Professor in the Cheriton School of Computer Science at the University of Waterloo. Michael A. Specter is an assistant professor of Computer Science at Georgia Tech. Douglas Stebila is a professor in the Department of Combinatorics and Optimization at the University of Waterloo, where he leads a research group in applied cryptography. Peter Swire is the J.Z. Liang Chair in the Georgia Tech School of Cybersecurity and Privacy. More detailed biosketches are provided at the end of this document.

This document concludes:

- (1) Over-broad regulations and orders would reduce security. Broad C-22 regulations could reduce the security of numerous types of systems, and the so-called “systemic vulnerability” exception would in fact create systemic vulnerabilities.
- (2) There are risks created by the bill’s one-sided procedures, creating a strong incentive for full compliance without question, even when the government request is beyond the actual scope of the law.
- (3) C-22 has significant weaknesses compared to the U.S. law from which some definitions have been drawn.
- (4) There are surprising lessons from a September Globe and Mail article about a phone that police could not access.

This document makes nine recommendations:

- R1. Close the loophole for risks that “relate only to” people under a warrant, following Australia.
- R2. Count weakened authentication or encryption, and the risk that information could be altered, as systemic vulnerabilities.
- R3. Extend the protection to hardware, software and systems, not only “services.”
- R4. Remove the test “based on recognized international technical standards.”
- R5. Restate section 2(4) in terms of access, so that it covers more than decryption.
- R6. Make the protection a limit on the government, so that an order has no effect to the extent it would create a systemic vulnerability.
- R7. Let providers obtain an independent technical assessment, reported to the Intelligence Commissioner, before an order is approved.
- R8. Require periodic independent review and public reporting, including on providers’ objections.
- R9. Adopt the rule from a similar U.S. law (CALEA) that the government may not prohibit a provider from adopting stronger security.

After drafting this document, we reviewed Google’s submitted [comments](#) to this Committee, which highlight many of the same concerns analyzed here.

Over-broad Regulations and Orders Would Reduce Security

Broad C-22 Regulations Could Reduce the Security of Numerous Types of Systems

Part 2 of the bill is entitled “Supporting Authorized Access to Information Act.” The bill creates a framework to order electronic service providers (ESPs) to provide law enforcement and intelligence access to defined information about users. Under the bill, the Governor in Council shall create a regulation applying to defined ESPs, called “core ESPs.” The regulation can define obligations for the “development” and “maintenance” of “operational and technical capabilities.” The regulation can also require the “installation” and “maintenance” of “any device, equipment, or other thing” that might enable access to information by authorized government officials.

Major concerns about C-22 apply to these potentially broad regulations to create “operational and technical capabilities” and install “any device, equipment, or other thing” to the messaging, email, and other services used by Canadians. A central part of the debate is how, and in what ways, these regulations will require service providers to enable access to encrypted communications. In the view of Commissioner Carrique, police “need the ability to get to that encrypted data.”

Based on our many years debating prior proposals to limit encryption, there are multiple, compelling reasons for the greatest skepticism about a law that would require service providers to change their services to give government access to that encrypted data. **Prior work shows that such a law is incompatible with state-of-the-art security practices.** It would dramatically increase system and operational complexity, raising cybersecurity risk. It would undermine forward secrecy, the cryptographic principle that past recorded communications should be protected from being decrypted even if a private key or password is stolen in the future. It would disincentivize others from adopting important protection mechanisms altogether.

A fundamental concern is that a system that is broken to assist Canadian law enforcement will also be broken in protecting against attacks from hackers and hostile governments. There is no way to design an encrypted communication system that enables “lawful access” without simultaneously introducing a systemic vulnerability that puts all the system’s communications at risk. Swire and Specter, in recent [scholarship](#) with Kenesa Ahmad, call this the “least trusted country” problem—a proposal by one government (such as Canada) to break an encryption system also lays the system open to attack from whatever other country (or private group) one trusts the least. **If Canada requires service providers to create “operational and technical capabilities” to break secure systems, then the same attack vectors are left open to others, globally.**

The recent Swire and Specter article explains in detail how **end-to-end encryption (E2EE) is now built into a large portion of the protocols used in modern computing.** Bill C-22 has received harsh criticism from suppliers of Virtual Private Networks (VPNs), with major suppliers saying they would withdraw from the Canadian market if the bill becomes law. Other potentially affected protocols would include: Transport Layer Security (TLS) and the Hypertext Transfer Protocol Secure (HTTPS), the principal protocols for web surfing; SCP (Secure Copy Protocol) and SFTP (Secure File Transfer Protocol), which rely on Secure Shell encryption (SSH), the protocols pervasively used for remotely-managed computing; and Zero-Trust Architecture (ZTA), the approach required for Canadian federal agencies as part of its Enterprise Cyber Security Strategy. ZTA uses strong encryption even between two computers in the same network, and would be undermined if the products and services it relies on had to build in “technical and operational capabilities” to gain access to encrypted communications. **All of these vital components of modern computing rely on encryption whose keys are held only by the communicating endpoints, not by the networks over which the traffic flows, leading to the conclusion that E2EE “is a feature of modern computing, and not a bug to eliminate or restrict.”** Where a provider is itself an endpoint, such as a web service that terminates TLS, it can already read the content, and an order would not need to weaken encryption to obtain it. The danger arises when an order requires a provider to give access to traffic that it carries but cannot read, such as an Internet or VPN provider carrying users’ TLS-encrypted web traffic; that can be done only by weakening the protocol itself, for everyone. **Broad C-**

22 regulations could thus threaten numerous, critical modern protocols, at a time when risks of cyber-attacks are multiplying due to the use of AI by nation state and other hackers.

Key Canadian agencies have recently underscored the importance of relying on well-encrypted systems. The Canadian Centre for Cyber Security and the Canadian Security Intelligence Service were signatories of 2025 [guidance](#) on countering the compromise of networks globally, often [referred to](#) as the “Salt Typhoon” attacks on telecommunication networks. The guidance was crystal clear about the importance of pervasively deploying effective encryption: “Only use encrypted and authenticated management protocols (e.g., SSH, SFTP/SCP, HTTPS) and disable all others, especially unencrypted protocols (e.g., Telnet, FTP, HTTP).” The Salt Typhoon attack reportedly took advantage of the systems that U.S. carriers had built under CALEA to carry out court-authorized wiretaps, the kind of capability that C-22 would allow the government to require providers to build.

The “Systemic Vulnerability” Exception Would Create Systemic Vulnerabilities

As Bill C-22 has progressed through the legislative process, there have been some welcome amendments that address some encryption concerns, but only partially. Notably, the updated bill states that a core provider is **not** required to comply with a government request “if compliance with that provision would have the effect of requiring the provider to introduce a systemic vulnerability related to that service.” **The bill defines systemic vulnerability as “a vulnerability in the electronic protections of an electronic service that creates a credible risk, based on recognized international technical standards, that secure information could be accessed by a person who does not have any right or authority to do so, other than a risk that relates only to information related to persons with respect to whom a warrant, order or other authority to access information conferred under the Criminal Code or the Canadian Security Intelligence Service Act — or any similar authority conferred under another Act of Parliament — applies.”**

With any proposed law, the devil is in the details. Here are five concerns with the current definition. **First**, the law applies to “systemic” vulnerabilities; however, **if a provider has to be able to target one user upon request, it has to build a system that can be turned against any user whenever it is told.** That ability is a systemic vulnerability, in our opinion and that of a clear majority of the security community. Once that ability exists, it can be misused by an insider or an attacker who compromises the provider. Yet the definition’s closing words exclude any risk that “relates only to” people under a warrant, inviting the argument that such a capability is not a systemic vulnerability at all.

Second, the exception appears to apply only to confidentiality, where “secure information could be accessed.” The Act defines “electronic protection” to include authentication as well as encryption, but the definition counts only the risk that information could be “accessed,” not the risk that it could be altered or that a user could be impersonated. **Confidentiality, however, is only one of the modern tasks for cryptography.** Cryptography today is used to protect the [integrity](#) of data (proving that data has not been changed). It also applies to “authenticated management protocols,” of the sort that the Canadian Centre for Cyber Security emphasized should replace the earlier, unencrypted approaches. **Stronger authentication protocols, relying on cryptography, have become increasingly necessary.**

A third concern is that most attacks on encrypted information do not attack the encryption algorithm; instead, they target how the algorithm is implemented in practice. In the [words](#) of

cryptography expert Bruce Schneier, “It’s far easier for an attacker to bypass cryptography by exploiting a vulnerability in the system than it is to break the mathematics.” The same is true of government mandates. An order could require a provider to secretly add a participant or device to a target’s conversations, to push a modified software update to one user, or to scan content on the device before it is encrypted. None of these breaks the encryption itself, but each defeats encryption as effectively as a backdoor would. **The definition does not make clear that such techniques count as systemic vulnerabilities, and it is unclear whether s. 2(4), which addresses only decryption, covers them (see R5).**

Fourth, the systemic vulnerability language refers to risks **"based on recognized international technical standards"**, but this **is not a good test**. International technical standards generally describe security mechanisms, not methods for assessing risks, and these standards are slow to develop, so they will lag behind new techniques. Moreover, there are some recognized standards that exist for the purpose of weakening encryption for access, such as ETSI's "Enterprise Transport Security"; the government could cite such standards to argue that an order meets international standards. When a provider and the government disagree about whether a risk is “credible,” an independent technical assessment (R7) can be called on.

Fifth, the scope of the definition of electronic service providers and core ESPs remains unclear, and could be read broadly to apply to consumer apps, operating systems, software developers, and cloud providers that provide services to Canadians. The Act defines an “electronic service” to include “a service, or a feature of a service,” and ministerial orders under s. 7(1) can be directed to any electronic service provider, not only to core providers. The systemic-vulnerability protection, by contrast, applies only to vulnerabilities in an “electronic service.” For example, in the context of Apple iMessage, one could argue that none of the iOS operating system, the iPhone device firmware, or the iMessage app on the phone is an “electronic service.” If so, Apple could be ordered to change one of them without the protection applying. **Regulations thus may interpret the definition of electronic service providers to be very broad, including far more than the traditional definition of “services.” At the same time the exception to the orders, for systemic vulnerabilities, is too narrow, as shown by the previous four points.**

These five concerns highlight ways that government mandates that undermine cybersecurity and privacy may be lawful under Bill C-22, despite the existence of the systemic vulnerability exception.

A related set of concerns arises from section 2(4), which says that no obligation under the Act is to be construed as compelling a provider to decrypt, or to ensure that an authorized person is able to decrypt, information its users have encrypted, unless the provider supplied the encryption and holds the information needed to decrypt it. Section 2(4) does not define “decrypt,” and it protects only providers that do not hold the keys. Although the bill seems to indicate that decryption will not be required, government orders could break security through multiple paths other than decrypting a communication. For instance, a regulation or order might require a core provider to enable interception on devices before the data is encrypted in transit, as in the case of proposals for scanning activity on the user’s device.

Several of the recommendations below draw on Australia’s Telecommunications Act 1997, as amended in 2018 by its Assistance and Access Act. That law is widely regarded as one of the most far-reaching lawful-access laws in any democracy, yet it contains safeguards that C-22 lacks.

Recommendations on the scope of regulations and the definition of “systemic vulnerability”:

R1. Strike the closing words that say that a risk doesn't count if it "relates only to" people under a warrant, and instead **adopt Australia's rule that a weakness aimed at one person is still considered systemic if it puts anyone else's information at material risk.**

R2. Adopt the Privacy Commissioner's [recommendation](#) that "systemic vulnerability" include "any action that would render systemic methods of **authentication** or encryption less effective", similar to Australia's law. Also amend the definition so that it counts the risk that information could be “accessed or altered,” not only “accessed.”

R3. **Extend the systemic-vulnerability protections** (the definition in section 2(1) and the provisions in sections 5(5) and 7(5)) **to hardware, software, and systems, not only services.**

R4. **Remove the clause "based on recognized international technical standards"** from the definition of “systemic vulnerability”.

R5. **Extend 2(4) beyond decryption, stating it in terms of access rather than particular techniques:** no regulation or order may require a provider to do anything that would give the provider, or anyone else, access to information that its service is intended to prevent the provider from accessing. Compelled decryption would then be one example, as would requiring a provider to add hidden participants or devices, access content on the device before encryption, send particular users modified software, or switch off encryption. Possible language to address this concern would be to state: “No obligation under this Act is to be construed as requiring an electronic service provider to do anything that would give the provider, or any other person, access to information (including data or metadata) that the provider’s service is designed to prevent the provider from accessing, including by decrypting the information or enabling an authorized person to decrypt it.”

R6. **State the protection as a limit on the government,** as the Privacy Commissioner recommended and as Australia does (Telecommunications Act 1997, s. 317ZG(1) and (5)): a regulation or order must not have the effect of requiring a provider to introduce a systemic vulnerability, or of preventing it from fixing one, and has no effect to the extent that it would. As drafted, the protection is an exemption that the provider must claim, at its own risk, against an order it cannot discuss publicly.

Risks Resulting from One-Sided Procedures

The discussion thus far has shown significant areas of uncertainty about the scope of mandates under Bill C-22, and the overly narrow scope of the systemic vulnerability exception. **We next examine how the uncertainty in C-22 tilts the field greatly toward the government, even when providers have strong legal and practical arguments that a request goes beyond what is authorized by the law. The current procedures create a strong incentive for full compliance without question, even when the government request is beyond the actual scope of the law.**

The procedures in Bill C-22 are asymmetric—the government can mandate immediate action, backed up by serious penalties, but the companies lack any similar ability to dispute an

overbroad order or gain an automatic stay while the order is being contested. Sections 19–46 of the Bill set forth a detailed description of the processes, mechanisms, and penalties available to the government to ensure compliance with regulations issued by the Governor in Council or an order issued by the Minister. These provisions account for every stage of enforcement against an ESP, from a notice of non-compliance to authorizations for broad physical searches of ESP premises, staged infractions, and fines that can lead to personal liability.

By contrast, the Bill contains no similar procedures for providers to challenge a regulation or order. Orders do require the Intelligence Commissioner’s approval before they take effect (s. 7(2)), but that review is of the reasonableness of the Minister’s conclusions, and there is no requirement to consult independent technical expertise. The timing of an order can be immediate, such as where there are “exigent” circumstances, requiring immediate response by the service providers. In the same article quoting Commissioner Carrique, Apple is quoted as saying that 35% of previous requests have been on this sort of emergency basis. More generally, the Minister can specify the day when compliance is due. By contrast, any individual seeking judicial review must provide the authorities with 15 days of advance notice before filing. **These asymmetric time periods for legal action appear to undermine the ability of ESPs to seek immediate relief, even on a temporary basis, from being compelled to take steps that could undermine the security and integrity of their users’ data and their infrastructure.**

The asymmetric procedures in the current bill create a difficult position for any provider who believes in good faith that an order actually creates a “systemic vulnerability” or otherwise goes beyond the government’s power to seek action. **Penalties can apply, even personally to corporate officers, before the 15 days pass that enable a challenge to the overbroad order.** Providers and their employees thus face strong incentives to comply immediately, even where there are valid legal reasons why the order goes too far.

Australia's act (section 317WA) allows a provider to request, prior to being ordered to build a new capability, an independent assessment by two people (a technical assessor and a former judge) to assess whether the order would create a systemic vulnerability. The assessors must give “the greatest weight” to the question of whether it creates a systemic vulnerability. The provider receives a copy of the report. If Bill C-22 were revised to allow this, the assessor's report should be part of the Intelligence Commissioner's input for deciding whether to approve an order.

Recommendations:

R7. Give providers a way to object. A provider that believes in good faith that an order would create a systemic vulnerability should be able to request an independent assessment, by a technical expert and a former judge as in Australia (s. 317WA), with the report going to the Intelligence Commissioner before the order is approved. While the assessment is pending, any obligation to build or change a capability should be suspended; obligations to disclose information the provider already holds would be unaffected. Such amendments would seem to uphold the intent of the current Bill, enabling orders while setting legal limits against over-broad orders that are contrary to the Bill’s intent and text.

R8. There should be periodic outside review and public reporting requirements, as exist for instance for wiretap orders and Section 72(2) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. The annual report under s. 49 should also state how often providers objected

that an order would create a systemic vulnerability, how often an independent assessment was requested, and how those objections were resolved.

C-22 Has Significant Weaknesses Compared to the U.S. Law From Which Some Definitions Have Been Drawn

One argument in support of Bill C-22 is that other countries, including the United States, also have laws that require providers to design their systems with the technical capability to access defined communications.

Such an argument is misplaced with respect to the U.S. Communications Assistance for Law Enforcement Act (CALEA), which creates a technical assistance regime that may seem similar to Bill C-22. The comparison with CALEA is particularly informative, because section 2(4) of Bill C-22, its limit on compelled decryption, is copied almost word for word from CALEA (47 U.S.C. § 1002(b)(3)).

First, **CALEA prohibits law enforcement from “requir[ing] any specific design of equipment, facilities, services, features, or system configurations to be adopted” and from “prohibit[ing] the adoption of any equipment, facility, service, or feature.”** In other words, unlike Bill C-22, which allows the requestor to dictate the time and manner of assistance, CALEA acknowledges that each in-scope service provider’s system will be built and function differently, and so any technical capability mechanisms that are required must be tailored to the needs of—and therefore designed by—each provider.

Second, CALEA applies only to telecommunications providers like phone companies and ISPs. Due to its exclusion for “information services,” its technical assistance obligations do not apply to services that operate at the application layer—CALEA specifically, for example, excludes “electronic messaging services.” As a related point, CALEA provides a clear carve-out from otherwise applicable technical assistance obligations in cases where encryption is applied by third parties. In the traditional phone system covered by CALEA, the law clearly exempted third-party encryption application-based services such as electronic messaging services or individual users. C-22 thus copied one of CALEA’s three safeguards, the decryption limit, and left out the two that limit design mandates and keep the regime away from Internet services. In short, the broad technical assistance provisions in C-22 are entirely unlike how the U.S. has proceeded since the start of the commercial Internet.

Recommendation:

R9. Although language in C-22 appears to track laws in the U.S. and other Five Eyes countries, **participants in legislative debates should recognize that there are multiple safeguards built into those laws that do not currently exist in C-22.** At a minimum, C-22 should adopt CALEA’s rule that the government may not prohibit a provider from adopting any equipment, facility, service, or feature, so that an order cannot stop a provider from introducing stronger security such as end-to-end encryption.

Surprising Lessons from a Globe and Mail Article

A September [article](#) in the Globe and Mail highlighted law enforcement concerns about being stymied by encrypted communications. According to the article, police were unable to access messages in a phone running an open-source operating system called GrapheneOS. The article cites the support of Bill C-22 by Toronto Police Chief Myron Demkiw. Although not commenting on any particular ongoing investigation, **a Toronto police spokesperson stated: “As criminals increasingly use encrypted technology to facilitate serious criminal activity, law enforcement needs the appropriate lawful tools to keep pace.”**

On closer examination, the reported facts about GrapheneOS actually illustrate limits and predictable downsides if Bill C-22 were to become law in its current form. The article noted that the encryption in GrapheneOS is open source—software chosen by the user, and not run by an ESP subject to the bill. It would thus appear that there would be no service provider, covered by Bill C-22, able to decrypt the communication and respond to an order. Thus, for criminals or others seeking to evade Canadian law enforcement, Bill C-22 would provide a clear incentive to shift away from current providers to open-source solutions. More generally, there will always be open-source or foreign-encrypted tools that remain out of reach of Canadian law enforcement.

This shift to foreign sources of encryption, beyond the reach of national authorities, has occurred previously. Swire [chaired](#) the White House Working Group on Encryption in 1999, when the U.S. decided to eliminate strict export controls on strong encryption. A significant reason for the shift in U.S. policy, toward supporting strong encryption, was the growing realization that continued limits on U.S. use of strong encryption would shift an ever-greater portion of encryption services to Russia and other nations. **The same dynamic would apply under Bill C-22, driving users away from Canadian-provided services toward open-source or foreign-supplied encryption.**

Conclusion

Strong encryption, including end-to-end encryption, is a feature of modern computing, and not a bug. **In our global communications networks, security cannot be maintained unless strong encryption is deployed in the numerous protocols on which modern computing depends.**

Since the 1990s, law enforcement and national security leaders globally have repeatedly proposed legislation that claims to provide access to encrypted communications while maintaining cybersecurity and privacy. In response, encryption experts have demonstrated again and again that **any mechanism letting a third party access properly encrypted content necessarily weakens security against all other attackers.** In the face of innumerable hacking attacks from nation states and other actors, even the best-intentioned legislation to weaken encryption confronts the central issue—mandated encryption flaws required by one country, such as Canada, open up attack vectors for the least trusted countries and bad actors in the world.

The authors have dedicated decades of work to the essential project of providing cybersecurity and privacy in a global, networked environment. Mandating weaknesses and flaws in encryption is not good public policy, as Canada’s own government agencies have recognized in their security guidance. **To the extent that C-22 moves forward, it is vital to provide improved definitions for “systemic vulnerability” and other terms, to make the systemic-vulnerability protection a binding limit on the government, and to give providers an independent technical**

assessment before an order takes effect. The current definitions, by contrast, risk serious harm to Canadian citizens, companies, and government agencies. They also create incentives for Canadians to rely more heavily on non-Canadian services and technologies, especially those outside the reach of Canadian jurisdiction.

Author Biographies

Ian Goldberg is the Canada Research Chair in Privacy Enhancing Technologies. He is a Professor in the Cheriton School of Computer Science at the University of Waterloo, where he is a founding member of the Cryptography, Security, and Privacy (CrySP) research group. He has been working and researching in the areas of cryptography, security, and privacy for online communication and computation for over 30 years, including in his role as Chief Scientist at Zero-Knowledge Systems, a Montreal-based startup. He is a Fellow of the Association for Computing Machinery, and was recently elected a Fellow of the Royal Society of Canada. He is a winner of the USENIX Security Test of Time Award, the Asiacrypt Test-of-Time Award, the Electronic Frontier Foundation Pioneer Award, and the Caspar Bowden Award for Outstanding Research in Privacy Enhancing Technologies.

Michael A. Specter is an Assistant Professor of Computer Science at Georgia Tech and director of the Security Privacy and Democracy Research Laboratory. Specter's research focuses on problems in systems security and applied cryptography, particularly on issues relevant to public policy. He completed his PhD in Electrical Engineering and Computer Science from MIT, and previously served as research staff at MIT's Lincoln Laboratory. His research has been featured in congressional testimony, amicus briefs to the Supreme Court, and (repeatedly) in the popular press. He holds a Research Award from the Elections Verification Network and a Pioneer Award from the Electronic Frontier Foundation.

Douglas Stebila is a professor in the Department of Combinatorics and Optimization at the University of Waterloo, where he leads a research group in applied cryptography. His research concerns the security of protocols that protect everyday online activity, including the TLS protocol used in web browsers and end-to-end encrypted messaging applications such as Signal. He co-authored the reference text *Protocols for Authentication and Key Establishment* (Springer, 2019) and served as program co-chair of CRYPTO 2024. He has consulted for technology companies, including Apple, which commissioned him to analyze the cryptography underlying its iMessage PQ3 protocol.

Peter Swire is the J.Z. Liang Chair in the Georgia Tech School of Cybersecurity and Privacy. For the past decade Swire has led a [university project](#) on law enforcement requests for data, and now is Research Director for the [Cross-Border Data Forum](#), a think tank that supports legitimate government requests for evidence while protecting privacy and cybersecurity. In 1999, he chaired the U.S. White House Working Group on Encryption. He has published extensively on encryption, including in testimony before the U.S. Senate Judiciary Committee, and served on the National Academy of Sciences Forum on Cyber-Resiliency.