Insight

Data Protection and the Pandemic: What We Can Learn for Future Policy

JENNIFER HUDDLESTON | APRIL 8, 2020

- As the United States considers federal data protection legislation, policymakers should consider how lessons from the pandemic illustrate the tradeoffs associated with stringent policies and the different choices individuals may make when it comes to their data privacy.
- Stringent data protection regulations, such as the European Union's General Data Protection Regulation, can hinder responses during an emergency like the COVID-19 pandemic.
- The potential benefits of using some less-secure technologies during social distancing outweigh the privacy and security risks associated with them, and the decision about the balance between these risks and benefits will be different for different consumers and situations.

Introduction

The ongoing COVID-19 pandemic provides a useful case study for the impact of privacy regulations. U.S. policymakers have been considering federal data protection legislation for some time, and whether the current less regulatory approach remains appropriate. The European Union's (EU) General Data Protection Regulation (GDPR) provides an example of a sweeping and highly regulatory approach to data privacy and security while the less stringent approach in the United States leaves more room for innovation, flexibility, and choice. The COVID-19 pandemic illustrates the tradeoffs associated with stringent policies and the different choices individuals may make when it comes to their data privacy, highlighting the value of a flexible and less prescriptive approach to privacy regulation.

The Impact of Data Protection Regulations on Pandemic Responses: Distinctions in the European and American Approaches

The COVID-19 pandemic has illustrated some of the unintended consequences that stringent data protection laws can have. Such policies prioritize strong data privacy and security over other concerns and potential benefits. But the social and business situations arising from the pandemic have shown that the risks associated with in–person meetings or the limitations of analog technologies may outweigh the risks of using technology or data that would be rendered difficult or impossible with heavy-handed regulations.

While officials claim the GDPR should not hinder the response to COVID-19, there has been an impact on certain technologically enabled responses as a result of the requirements and restrictions regarding individuals' data. EU guidance on GDPR and the pandemic requires member countries to pass legislative exceptions to allow responses using location information or employment information, exceptions that would not be necessary in other countries including the United States. Stringent data privacy regulations can also place burdens on b usinesses transitioning to remote work that must consider the concerns of GDPR compliance for data and document transfers and the risk of security breaches. The regulations are also increasing burdens on innovative and charitable responses. For example, in the United Kingdom, grocery stores seeking to deliver food boxes to 1.5 million vulnerable individuals were

unable to receive the needed information due to GDPR "protections" against the mass sharing of personal information such as individuals' names, addresses, and emails. GDPR's limitations on such data sharing also make it more difficult for developers seeking to create an app that could help with contact tracing of individuals with COVID-19.

In general, the United States already had a less regulatory approach to data protection than the EU, and this distinction has become even more apparent in the decision to lift certain data protection restrictions during the pandemic. Loosening certain requirements around the Health Insurance Portability and Accountability Act (HIPAA) has enabled the broader use of telemedicine via publicly available messaging and videoconferencing services such as FaceTime and WhatsApp. Telemedicine is playing an important role in preserving limited health resources and allowing triage and the continued social distancing for certain needed visits. As with other regulations removed during the pandemic, policymakers should carefully reexamine if they were truly needed before reinstating such restrictions.

Policymakers should consider that the consequences of stringent data protection regulation might prevent other benefits including the potential innovative responses to emergencies like COVID-19. While at times regulation may be necessary to prevent harm, such regulations presume that minimizing data privacy and security risks should always be the priority. The pandemic has illustrated that such an approach has its own risks and harms , and individuals and private institutions are often in a better position to weigh the risks and make decisions that fit their own circumstances

Data Protection Preferences and Tradeoffs: Considering Concerns About Zoom, Privacy, and Security

Videoconferencing services have become increasingly popular particularly for individuals who have to work or attend school from home. While a variety of options are available, Zoom has quickly risen to become a household name. But along with its meteoritic rise, Zoom is facing new questions about the data security risk it may pose and its privacy policy. A class action lawsuit was filed against Zoom in California alleging it improperly shares user data with Facebook, and the New York Attorney General is investigating the company's privacy practices as well. Senator Sherrod Brown has requested that the Federal Trade Commission (FTC) investigate whether the company's claims regarding the encryption of its services were deceptive. Some headlines have even gone so far as to refer to Zoom as malware.

While some policymakers clearly are uncomfortable with the relatively lax security around Zoom calls, again a sweeping and highly prescriptive policy will not balance the many needs that consumers have. As Columbia University Computer Science Professor Steven M. Bellovin notes in an analysis of the security risks associated with Zoom, when it comes to data security risks, concerns should consider the benefits of use, the potential incremental risks from use, and if anything can be done to minimize those risks. In many cases for consumers and business, the availability of free or low–cost and easy to use videoconferencing services are of a greater benefit than the potential risks of in–person meetings or more analog options. But as with most data privacy issues, there are different needs and preferences when it comes to data security and privacy for video conferences. In many cases, these preferences may vary with the purpose of the use or the sensitivity for the information. For example, businesses conducting more sensitive business, such as a meeting involving financial transactions or trade secrets, may prefer heightened security of encrypted options such as WhatsApp or FaceTime. Individuals may find they desire the higher level of security or privacy from an encrypted service when discussing more sensitive issues, such as their health on a telehealth visit. In contrast, however, the risks of Zoom may not outweigh the cost and ease of use of Zoom for chatting with a book club or conducting a virtual happy hour.

All options have tradeoffs, whether it is data security, the limitations of the technology, or the risks of an in-person meeting

. For example, FaceTime cannot support as many users on a single call as Zoom and so may not be an option for larger meetings, while an analog option such as phone calls may make it more difficult to properly convey information. As a result, consumers and businesses find themselves weighing risks and benefits of different options. When the situation changes, the risks and benefits will as well, and so might the choices that are made.

Enabling a wide range of services rather than dictating specific practices will also allow responses to consumer demands. Zoom, for example, switched its defaults to include passwords and waiting rooms in response to consumer concerns over "Zoom bombing" (uninvited guests appearing in Zoom meetings). By not requiring specific responses, barriers to entry remain low and can allow new competitors to offer solutions for the specific privacy or security concerns. Companies should provide transparent and honest information about the privacy and security of their software, including if meetings are encrypted and the use of data. Individuals and businesses should also follow common sense and data security best practices. For example, they should be cautious of sharing screenshots where access codes or passwords for meetings are publicly shown.

A Better Way to Regulate

The COVID-19 pandemic is illustrating why it is important that policymakers and consumers consider both risks and benefits when it comes to data privacy and security. For many, the benefits of using Zoom or similar technologies currently outweigh the risks and consequences associated with the alternatives. A highly regulatory approach to data protection prioritizes privacy and security in a way that can create burdens for innovative response both during an emergency and beyond. Such an approach presumes that data privacy and security is always the highest benefit to consumers, when there are often many more factors and risks involved. The advantage of the current approach to data protection in the United States is it allows consumers and businesses to make the choices that reflect their preferences rather than the government presuming that greater privacy or security is always the right benefit.

The United States' current less-prescriptive approach does not leave consumers without redress where there are problems. In cases where information is deceptive or harmful to consumers, existing enforcement options are available through the FTC and consumer protection actions from state attorneys general. This approach can provide information and empowers consumers and businesses to make the choices that best reflect their risk preferences. Ideally, these lessons will lead to more nuanced conversations about the benefits and consequences associated with data privacy regulations as policymakers continue to debate the need for a federal data protection framework.