
TOP FIVE UNANSWERED PRIVACY QUESTIONS FOR LAWYERS

JAY CLINE
AUTHOR

ABSTRACT

The judicial system makes decisions that shape and define the way we live, and the ambiguous territory of privacy is one area that begs for clearer definitions. There are legal questions that need to be answered in regard to privacy including: What is privacy? How should a breach of privacy be compensated? What is consent for use of personal information and when is it necessary? Society needs the help of lawyers to answer these new and important questions.

Top Five Unanswered Privacy Questions for Lawyers

By Jay Cline

People joke about lawyers, but I think many people *secretly desire* to become lawyers. The phenomenal success of the TV shows *Law & Order* and *Boston Legal* show how much we laymen vicariously live through the legal profession on a daily basis. But what explains this? Is it the raw attraction of seeing the slam of the gavel send a criminal to his fate? Maybe so.

But I think a second factor is at work in many of us. It's the drama of watching the judicial system attempt to answer the toughest questions of society in a way that will redefine how we live together thereafter. And in this age of terror, there's a critical drama unfolding before us over the questions of personal privacy. Lawyers who can help answer five core questions about

privacy will be making a valuable contribution to society.

Cline manages data privacy at Minneapolis-based Carlson Companies. These views are his own and do not necessarily reflect those of Carlson. He can be reached at privacy@carlson.com.

1. What Is "Privacy"?

This sounds like such a basic question, but we really haven't figured it out yet, either in the United States or globally. And it's resulting in a patchwork of state, federal, and international privacy laws that are often at odds with each other. We need to answer this question.

Some say privacy is the right to be left alone. Others say it's the ability to control the use of your personal information. In the national privacy laws of Canada, EU member states, and Australia, privacy is defined more broadly to be based on a set of eight to ten key principles.

Here in the States, we've let this

question get deeply entangled in the abortion debate. Pro-choice sympathizers are inclined to answer the question "What is privacy?" in a way that includes the right to abortion. Yet this doesn't help any of us in the data-privacy profession. What happens if the new Supreme Court of the United States overturns *Roe v. Wade* and its underlying privacy arguments? Will we go backward on our data-privacy protections in the United States as well? We need smart lawyers who can define what privacy means in an honest, unbiased, and universal way.

2. What Is "Harm" When Privacy Is Violated?

Our American courts have had difficulty awarding victims of privacy breaches any substantial compensation. Beyond the tangible damages for fraudulent credit card charges, lost work time, and attorneys' fees, judges have been reluctant to establish any meaningful precedents for compensating for the intangible effects of lost privacy.

This shouldn't be surprising because, to begin with, we don't even know what privacy is. Without knowing what the definition of privacy is, we won't know when it's been lost or

what the harmful effects of that loss will be.

It's one thing, for example, to receive an email or piece of postal mail you didn't ask for. It's hard to see any significant harm in that. But it's quite another matter to have your Social Security number or personal details posted to a website for the world to see. It seems like this is a graver situation than mere emotional distress. So, we in the privacy profession need a clever attorney to define how this kind of a situation would be a real, tangible loss for a person—or not.

3. What Is “Consent”?

The debate over whether privacy legislation should be “opt in” or “opt out” has evolved into a religious article of faith for many of the debate participants. Privacy watchdogs insist that people be asked for their opt-in consent for any uses of their personal information. Corporations, on the other hand, demand the flexibility of using personal information until people opt out of certain uses. We need a new voice in this debate to bridge these differences with an innovative answer.

For what uses of our personal information should our consent be sought?

Sending marketing communications to us? Sharing our information with unaffiliated third parties? With affiliates, too? Transferring it across borders? Using it for secondary, unrelated purposes? We need a framework to answer these questions.

Also, what form can consent take when it comes to information privacy? Is a written signature or checked-off box needed in all cases? Or would making a purchase or completing a process be sufficient indicators of consent in some cases?

For example, which of these two situations indicates more consent: the person who affirmatively clicks “I

agree” to a five-page Terms and Conditions that includes one oblique phrase addressing the right to email market the person? Or a person who provides an email address when purchasing a service that is commonly known to involve sending email marketing to customers?

Whoever can help us define what privacy is will be well positioned to show us how to think about consent.

4. What Is “Reasonable Security”?

Closely related to the use of information is the protection of information. Every national privacy law has a section addressing information protection, although these sections are sometimes entitled “data security” or “information safeguards.” They all say about the same thing: that companies must take “commercially reasonable measures” to prevent unauthorized access, alteration, or exposure of personal information. The Federal Trade Commission (FTC) has even started to pursue companies that aren’t taking

reasonable information-security measures.

But what does “commercially reasonable” mean? There are no definitions on the FTC website, and if you ask information-security professionals, they’ll tell you that it all depends on the situation. They’ll really resist attempts to define a one-size-fits-all approach to information security. For example, if you limit access to your most sensitive information to only three people, you might not need to encrypt the data at rest, unless there is Internet connectivity to that data. Situational logic can drive what securi-

ty measures are needed.

Nonetheless, the private sector is in great need of a blueprint that outlines its legal liability in this area. We need someone with a legal mindset to define a minimum set of security standards that, if a company deploys them, will be recognized by the courts to be taking reasonable measures.

5. What Is a “Breach” of Security?

The proliferation of security-breach notification laws at the state and federal levels has brought this question to the forefront. Companies are struggling to make good-faith efforts to update their incident-response plans to be in compliance across the United States. Their struggles stem in part from the fact that different states have codified different meanings of what a security breach is.

Some states say a breach is merely an exposure of personal information where an unauthorized person had the potential to steal it and use it for harmful purposes. Others say a breach is the unauthorized acquisition of per-

sonal information. These sound like semantic differences, but they can and are having a dramatic impact on how companies perceive and manage their risk in this area.

For example, if an employee finds a personnel file lying in the lunchroom, is that a security breach whereby all people whose information is in that folder need to be notified? Is it a breach if an information technology person temporarily places a file in a part of the network accessible by anyone on the Internet? Is it a breach if an employee emails an unencrypted spreadsheet of credit card numbers to an authorized person outside the company network?

The private sector, and I would

argue consumers as well, need this issue to be resolved before we start receiving in the mail so many notices of security breaches that they lose their meaning and impact.

Lawyers take a lot of flak, but at least in my profession, there is a great amount of respect for the contributions they have made and are making to help improve society in the area of privacy protection. These are the five core issues, in my opinion, with which we need your help. ♦

Top Five Unanswered Privacy Questions for Lawyers

First published in Vol. 3, No. 1, Summer 2006 of *SciTech Lawyer*,
a publication of the Section of Science & Technology.

About the Section of Science & Technology

The mission of the ABA Section of Science & Technology Law is to provide leadership on emerging issues at the intersection of law, science, and technology; to promote sound policy and public understanding on such issues; and to enhance the professional development of its members.

<http://www.abanet.org/scitech/home.html>

About ABA Publishing

ABA Publishing is a division of the American Bar Association (ABA), responsible for providing professional publishing guidance to both the association and its members. Our legal publications support professional excellence and greater understanding of the law. We publish approximately 100 law books per year as well as approximately 60 magazines, newsletters, and journals in numerous specialized areas of the law.

Our law books provide the best practice tips and pointers, sample forms and language, and professional legal guidance from experienced practitioners and are available in a variety of formats, including print, PDF, audio, and CD-ROM. Our authors and editors are outstanding professionals who are active in their fields. Experts rigorously review our products to ensure the highest quality information and presentation.

Articles

Individual articles are available as PDF downloads at www.abanet.org/abastore/index.cfm

For customer service, call 1-312-285-2221

Monday-Friday, 7:30-5:00 CST