



Data Privacy Detective Podcast – Episode 5 – Top Tips On Protecting Your Data

Nov 22, 2016

Categories:

[Blogs](#)

[Podcast](#)

[Publications](#)

[Technology Blog](#)

Authors:

[Joseph J. Dehner](#)

DPD: This is your Data Privacy Detective, sitting here with Julia Montgomery. Julia is a senior change management consultant at a company called [Traveling Coaches](#). Julia, tell us a little bit about what you do.

J.M.: Well, for the past few years, specifically, I've been focused almost entirely on working with law firms across the country to help educate their employees about information security and data privacy best practices.

DPD: Law firms probably better be secure with their data, so anything you are going to say about law firms, would probably be applicable to almost any business, any individual, would you say?

JM: Absolutely, one of the things that I tell law firm employees is that even though the focus of our program and our discussions is really about client information, the good habits that you pick up, learning to protect client information – sensitive confidential data – help you at home, too, to protect your personal information, your social security number, your credit card information.

DPD: We have devices everywhere communicating, PCs, wristwatches, automobiles now full of devices. I have heard there may be 50 billion devices by the year 2020. Let me ask you, Julie, what are your top tips for people and businesses for protecting their personal and business data?

JM: The most important thing, which is really the heart of the On Guard program, is information security awareness. We all know the world has changed, whether from the use of mobile devices or the internet of things. We have smart houses and smart cars. I think the issue is awareness of that. Be an informed consumer and user of these technologies.

DPD: Let's pause a moment and focus on email. A lot of us have gmail accounts and business accounts. What is your advice for email?

JM: When we sign up for these services, we agree, agree, agree our way through 14 pages of microscopic text. Somewhere in the middle of all of that we agree to relinquish certain rights to our privacy. We give providers like Google or Yahoo rights to access our information that we are trading for the conveniences of using their servers. To be clear, I am a user of these services, but I make sure to read the terms of service and understand what I'm agreeing to.

DPD: Let's be real. We all want the service and of course will click "I agree" so what should we do after we read through the conditions and agree?

JM: There are different degrees of information. I am willing to give access for example (though my mom would kill me) for Google employees to have access to my grandmother's pumpkin pie recipe. So I'll gmail that my sister. However, I recently purchased a home and both my closing attorney's office and my mortgage manager wanted me to send a form to them through my gmail account. The form included my Social Security number and banking account number. That is not information that I am willing to give Google access to. I don't want that to be on their servers, so I used an educated decision and used a different tool to send that information.

For more information, please contact [Joe Dehner](#) or any attorney in Frost Brown Todd's [Privacy and Information Security Law Practice Group](#).

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.