SRLN Brief: Court Technology Standards & Cybersecurity Considerations (SRLN 2019)

SRLN Justice Tech Working Group Call Summary

The Court Technology Standards and Cybersecurity Considerations discussed in the summary document attached below were topics of the Self-Represented Litigation Network (SRLN)’s Justice Tech Working Group’s December 13, 2019 webinar. On that webinar, Jim Harris discussed the JTC’s Court Technology Standards and Jason Tashea discussed cybersecurity practices technologist ought to consider in their work. The webinar recording and presentation slides can be access through the links provided in the summary.

Court Technology Standards

Technology is a disruptive tool that can amplify access to justice efforts across jurisdictional and physical boundaries. As a mechanism for automation, information sharing, and improving justice system interfaces, technology plays a critical role in expanding access to legal information, and products and services that deliver legal help to the public. There is no single technology solution that can address every justice system technology need, however. Instead, technology solutions should be designed to thrive in module-based environments. One framework that promotes this approach is the Court Technology Component Model that emphasizes the use of application program interfaces (APIs) and interoperability between products.

This framework was developed by the Joint Technology Committee (JTC), whose mission it is to improve the administration of justice through technology. The JTC was established by the Conference of State Court Administrators (COSCA), the National Association for Court Management (NACM), the National Center for State Courts (NCSC), and supported by the Integrated Justice Information Systems (IJIS) Institute. Together, these organizations convene court professionals and technology vendors to inform the development of standards that can be used to support technology adoption in courts across the nation. The JTC's Court Technology Standards Application Component Model speaks directly to the idea of module-based technology environments and advocates for designing court technology infrastructures able to function as a mosaic of products rather than a monolithic system. Standardizing court technology and promoting interoperability between technology products and services helps create a plug and play legal services ecosystem in which start-ups and incumbents can easily participate.

The Component Model is one of many projects supported by the JTC, and court technologist and vendors are encouraged to explore the array of publications that address standardizing technology. The JTC has identified several priority topics that are based on the Component Model framework and that include the OASIS LegalXML Electronic Court Filing (ECF) Specifications, the Online Dispute Resolution Technical Interface Standards, and guidance on Litigant Portals.

Building these standards as components to a court's technology infrastructure allows vendors to specialize and focus on certain aspect of a courts' technology needs. Moreover, these standards provide a roadmap that differentiates these products with enough specificity that innovation can happen without the need to

reinvent an entire digital system. By effectively utilizing APIs and interoperable inputs, vendors and courts alike are able to break away from single vendor services and instead build portfolios of technology services that address their specific jurisdictional needs. This in turn allows vendors to innovate and build expertise around a specific set of products, rather than having to build entire technology systems from the ground up.

For more information about Court Technology Standards, please visit the JTC Court Technology Standards page.

Cybersecurity Considerations

The adoption of digital systems that help manage court cases and allow court users to access and file case documents remotely necessitates a discussion about how these digital systems protect against cyber threats. One factor involved in utilizing technology solutions is appreciating that cybersecurity considerations should be part of any technology implementation plan. Both technology vendors and justice providers must contend with legal and ethical standards when deploying and designing technology solutions.

Courts, legal aid, and other justice system stakeholders often interact with litigant personal information across the continuum of services they provide–from basic legal information to full representation. To access court services, for example, a litigant might be asked to provide personal identifying information such as a home address, their social security number, financial information, health information, and the identities of minor children. Keeping this information confidential is both a legal and ethical requirement, but also impacts a persons' ability to seek safety from threats like domestic abuse, a contentious divorce, or stalking.

Technology providers, on the other hand, must consider the implications their technology solutions have on their duty to secure the data they collect, store, and use. Whether it is facilitating online filing, developing a services portal, or enabling automated document assembly, vendor technology designs must satisfy the standards courts, legal aid, and other justice system stakeholders are obligated to meet. Moreover, in addition toany state and local laws that apply to the use and collection of data, vendor practices must account for an array of federal laws specific to certain types of data, some laws to consider are provided at the end of this brief.

Some threats the justice community should seek to better understand, and technology providers should better defend against, are ransomware attacks, data breaches, undiscovered bugs in technology systems, and vulnerabilities caused by human error. Common efforts to guard against some of these threats include training staff[1] and providing guidance to spot and alert personnel about phishing attacks, updating passwords, using password managers, and tracking devices used by staff. Another practice the technology industry has developed and justice providers can require from[2] their vendors is implementing a vulnerability disclosure program. Finally, when appropriate, technology vendors might utilize bug bounties[3] to ensure ongoing system improvements to address security flaws.

For more information and news relating to cybersecurity, consider signing up for Jason Tashea's Justice Tech Newsletter at justicetech.substack.com.

---

[1] The Federal Trade Commission has developed guidance on recognizing and avoiding phishing scams.

[2] The United States Department of Justice Cybersecurity Unit has published white papers and research material outlining the value, use, and framework for developing vulnerability disclosure programs and policies.

[3] These programs authorize outside actors to notify a technology provider of bugs in their systems. Without these programs, well-intentioned third parties risk violating federal laws by disclosing these flaws through their unauthorized "hacking". In a report issued 2016, the United States Digital Service describes a bug bounty program developed by the Department of Defense's Digital Service team and outlines its impact, criteria, and lessons learned.

Federal Data Laws

Some data privacy laws that apply to technology services include:

- Federal Trade Commission Act of 1914 (FTC) (15 U.S.C. § 45) – the general application of the FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce. While not specific to a type of data, this law has been enforced against companies that handle personal information in ways that contradict their stated privacy policies and statements, or inadequately protect against unauthorized access or disclosure of personal information they promised to secure.

- Fair Credit Reporting Act of 1970 (FCRA) (15 U.S.C. § 1681 et seq.) – regulates consumer reporting agencies and consumer credit reports. The FCRA lays out how credit reports can be used and imposes obligations on those collecting, furnishing, or using a consumer's credit report.

- Health Insurance Portability and Accountability Act of 1996 (HIPPA) (42 U.S.C. § 1320d-6) – regulates the collection and disclosure of patient health information and requires providers of health data to have safeguards to protect against unauthorized use or access.

- Children's Online Privacy Protection Act of 1998 (COPPA) (15 U.S. Code § 6501) – regulates the online collection and use of information of children under the age of 13 and requires covered entities to post privacy policies, obtain verified parental consent, and to establish and maintain reasonable procedures to ensure the protection of confidentiality, security and integrity of any information collected.

- Gramm-Leach-Bliley Act of 1999 (GLBA) (15 U.S.C. § 6801) – regulates the protection of consumers' nonpublic personal financial information and records and requires financial institutions to implement safeguard and security measures to protect consumers' sensitive data.

Visit the SRLN Justice Tech Working Group for a summary of previous topics.

Last updated on December 10, 2020.

Year published: 2019

Document Author:

- Eduardo Gonzalez

Topics

Working Group Content

Regions

United States

Files

Call Summary–Court Technology Standards & Cybersecurity Considerations (SRLN 2019).pdf

SRLN Webinar Court Tech Standards and Data Security Considerations_Jim Harris.pdf

SRLN Webinar Court Tech Standards and Data Security Considerations_Jason Tashea.pptx

Print

Table of Contents