Digital Public

Contracting Digital Services for Courts

May 2022

Table of Contents

Introduction: Digital Transformation

While the digital transformation of courts has been under way for some time,[1] the response to the COVID-19 pandemic has driven a massive shift to digital services. There has been rapid implementation of case management software, remote hearing platforms, electronic filing, and digital evidence, to name a few. The speed and necessity of the shift to digital services[2] also meant building, procuring, and/or contracting relationships with digital service providers[3] with that same sense of urgency.

The National Center for State Courts, in partnership with a range of stakeholders, has produced several guides aimed at helping courts and aligned service providers address critical aspects of courts' digital transformation, including:

- Open Data Principles to Promote Court Technology Post-Pandemic
- Court Statistics Projects' Data Governance Policy Guide
- Guiding Principles for Post-Pandemic Court Technology

Introducing multiple digital services and digital service providers into a court's process can produce significant complexity that must be considered when contracting for those services.

This white paper is designed as a complement to the previously-released resources, focused on helping courts and court personnel to begin to incorporate the principles and approaches linked above into the contract terms that define their digital infrastructure.[4] Whether a court is in the beginning, middle, or end of a relationship with a digital service provider, this document will help a court identify potential issues, negotiate for better terms, and sign more effective contracts for digital court services.

This white paper is organized in three parts:

1. A review of the status quo of digital contracting
2. Defining procedural principles for procuring digital services
3. An overview of common digital contracts and considerations for courts

[1] Digital transformation means the move from paper-based processes to digital ones. Examples include: electronic case management systems instead of paper files, online dispute resolution and e-filing platforms, and virtual hearings.
[2] Digital services are things like e-filing, virtual hearings, electronic evidence, electronic case management systems, and online dispute resolution.
[3] Digital service providers are companies that help courts to offer those services via their technical expertise and/or software platforms. A vendor that supplies a court with an electronic case management system, for example, is a digital service provider.
[4] Digital infrastructure means the collection of software, hardware, and people that enable courts to provide digital services. For example, the internet service provider, the electronic case management software, and the in-house information technology department are all part of a court's digital infrastructure.

The Status Quo Paradox

The status quo for popular digital contracting is often not designed with the unique, publicly important needs of court systems in mind and, as a result, presents a range of litigant rights-affecting questions for courts' use of commercial digital services. For example, courts cannot choose their users and need to be able to interact with all people that engage with them. This situation incentivizes courts to use the most popular communication technologies – and yet, the more commercially popular a technology is, the less likely it is to be uniquely suited to a court's desire to meet litigant needs. For courts that presents a paradox: when considering the use of a technology, should a court prioritize using popularly available commercial services, which intermediates commercial actors into the administration of services, should they choose niche commercial services that might be less popularly-available, or should they try to build and host their own, which likely limits their accessibility while requiring significant, ongoing maintenance? None of these extremes is desirable for courts – courts are unlikely to be successful being fully dependent on commercially popular services that are not fit-for-purpose, nor will a court be successful building, hosting, and maintaining a totally independent technology 'stack' with no connection to commercial technologies. Digital tools need nearly constant updating and maintenance, meaning that any initial investments in technology will also require ongoing work (and resources) to keep them operating as intended.

The middle ground for most courts, currently and historically, has been to develop solutions through a combination of procured tools and contracted services. The challenge presented by the speed of digital transformation during the COVID-19 response is that court systems may not have had the time to establish appropriate technical standards or negotiate for the rights and relationships they typically require from commercial partners. Consider, for example, the number of courts that began using a given off-the-shelf remote video platform found that there were concerns with litigants' access, security concerns, or other concerns, shifted to a different platform, and ultimately engaged with an enterprise version of their original choice, all within the span of several months. In the absence of those standards and negotiations, many court systems have engaged technology partners whose interests are not perfectly aligned with the types of relationships courts have with their employees, legal service partners, or litigants. While there is nothing inherently wrong with partnering with unaligned service providers, the lack of alignment can increase the importance and impact of the contracts that define those relationships – and what happens when they go wrong.

The guides linked above lay out a vision for the digital transformation of court services – focused primarily on what systems should be able to deliver in terms of impact (neutrality, procedural fairness, etc.). In practice, those outcomes are the product of well-managed relationships between courts and service providers, as well as between courts and their stakeholders. **Relationships are especially visible in digital contracting because data and software systems are, themselves, mechanisms for managing service relationships.**

To illustrate this point, compare a home mortgage contract to a contract with a case management system vendor. The homeowner must pay the lender, but the lender doesn't have to approve

cosmetic changes to the house like painting a wall, nor does the homeowner depend on the lender to come and actually paint that wall. In contrast, a digital services contract could very well lay out exactly who can or cannot make a change to a software platform, like a case management system, even for aspects as minor as color scheme or font. It might also dictate who owns the data stored in that platform or who can make changes to the functionality of the platform, even changes that a court could have the ability to make on its own. In other words, a court might not be able to paint their own wall.

Digital services contracts not only require courts to define the authorities in the commercial relationship but the authority of each party to influence the relationships impacted by the use of data and technology. Rather than focus on the ways that digital services can go wrong, this white paper focuses on contracts as the instruments of those relationships and draws attention to the provisions necessary in those contracts for courts to be aware of, engaged in, and capable of governing their digital rights.

Procedural Principals for Digital Transformation Contracting

The most important set of rights for court systems to include in digital transformation contracts are procedural rights (who can paint that wall - the process for making changes to software, the process for addressing security issues, etc.). For the most part, public discussion around digital rights in courts has focused on the substantive application of rights – whether privacy rights, intellectual property rights, or employment rights. Substantive rights are important foundations for any digital, public system – but, as courts know all-too-well, rights are only as good as the parties' ability to enforce them. Too often, digital services contracts are crafted in ways that complicate, if not prevent, effective rights enforcement. Those complications are not based on substantive disagreements, they are based on procedural provisions and rights (or lack thereof) that prevent meaningful action on any issue. For example, the substantive right of an unhoused person to respond to a complaint via an online dispute resolution platform could be impacted by a court's lack of a procedural right to modify a mandatory address field in that platform to reflect that a person is unhoused. As a result, this guide focuses first on helping courts establish a contractual baseline of digital procedural rights.

Digital contracts are different than the contracts in other industries in at least a few, structurally important ways: (a) they are designed to avoid the complexity of contextual use, meaning that they rarely make affirmative warranties or guarantees about the integrity or fitness of a product for a particular use; digital contracts are framed around "all acceptable uses," as determined by the service provider; (b) they typically over-apply boilerplate contracting rules, by extending them into long-term contexts and creating unilateral amendment authorities; and (c) they often include provisions that divert litigation to arbitration or otherwise limit the means of redress available to users. The combination of these factors can make it challenging to negotiate with digital service providers during contracting.

Digital contracts are not different in the ways most often put forward by industry – it is not that they contemplate unsolvable problems or involve powers too innovative to limit – it is that they are typically designed to avoid any source of potential friction. This is often presented as a pitched battle for progress against inefficiency, but the most common types of problems with digital systems are not grandiose or unique, they are mostly banal – it is far more common for a product to stop working, a service provider to go out of business, or for a product to replicate predictable bias, than it is for court software to get caught up in a scandal. Though those problems can sound run-of-the-mill when described as technology problems, when they impact the way a court delivers services, those seemingly banal issues can result in a wide range of injustices.

Contracting the Status Quo: In February of 2021, whistleblowers revealed that the Arizona Department of Corrections' inmate management software was unable to account for a change in sentencing policy, and, as a result, was keeping hundreds of inmates in prison beyond their release date. Not only was the software error resulting in a fundamental loss of freedom using the state's power, it was costing the state significant amounts of money that weren't covered under their services contract. According to news coverage, senior Arizona Department of Correction leaders were aware of the problem for more than 2 years, before the story became public. While there is some dispute as to what issues were caused by software bugs and which were caused by configuration issues, the software system cost the state $24M and **many of the reported bugs weren't addressed because the Department of Corrections hadn't procured enough of the vendor's custom development hours in the contract to provide continuous updates.**

Courts should consider these principles for procedural rights in digital contracting:

Licenses, Limitations, and Granularity

Most digital contracts use open-ended licenses to define the parties' rights to data instead of articulating granular, limited uses. The open-endedness of data licenses can make it harder to establish and enforce reasonable limits on use, potentially putting the burden on a court system to monitor the service provider to ensure reasonable compliance. Even worse, these open-ended licenses can actively frustrate the transparency of the process and accountability for errors that effect court users.

The Dangers of Open Data's Long, Commercial Tail: One of the unintended consequences of courts' approach to opening data has been the emergence of data brokers who use criminal history to target commercial services or, worse, bias other services. This kind of digital appropriation is bad for litigants in a range of ways: (1) it opens people up to commercial exploitation during a vulnerable period; (2) it is often used in ways that bias future decisions by increasingly data-driven systems, like job candidacy, credit eligibility, or insurance premiums; and (3) it significantly limits the effectiveness of expungement – practically, and as a policy goal. While courts may be under statutory obligation to create public records, they still must do so in a way that is mindful of possible abuse at scale, in-part because licensing of underlying data can allow indiscriminate commercial use.

For example, a sealed criminal record could nonetheless become part of data that is sold and used by third parties, with serious consequences for the court user, even though the law and public policy concerns have attempted to make that information inaccessible to mitigate harm. Therefore, when contracting with software providers, courts should take care to delineate the rights and ownership of data captured within that system at the contracting phase. The contract should be explicit about which parties have the authority to license and/or sell specific kinds of data. Contracting should also consider the degree to which information captured within the system falls within the purview of open records requirements, which may apply to some data elements, but not others, and take care to not grant rights to data that are broader than intended or more permissive than the law requires without careful consideration.

Reporting and Supply Chain Transparency

Digital services are often the result of a combination of technologies – including software, data services, and web-hosting tools. Each unique service in a court's 'stack' adds a new actor to understand and, in some cases, to monitor. Courts that want to ensure their ability to enforce their users' rights – not only reporting and transparency information about the whole technology 'stack' – need to clarify the responsibility for ensuring and enforcing compliance across the supply chain of actors providing digital services.

Impact-Adjusting Diligence, Implementation, and Accountability

Court services typically operate at a higher standard than others, in part because of the recognition of how important they are to individuals' freedom and well-being. Courts, therefore, must ensure that those standards are met in contracts and procurement processes.

The three parts of the procurement process where these issues are most important are: (1) considering the potential impacts of failure to identify the due diligence requirements for prospective providers; (2) ensuring that courts' standards of practice pass through to service providers; and (3) acting as a guarantor of the accessibility of appropriate redress to court stakeholders, whether employees, attorneys, or litigants. Court systems are designed to protect a range of rights that are not effectively redressed through the

remedies provided by status quo digital contracting, and so it is critical that courts consider the pathways to enforcement for those who may be impacted by digital services' implementation and transformation.

New Case Management Software, Part 1: In 2016, Alameda County shifted from its legacy case management system to a new one, a transition that was not properly planned, resulting in thousands of rights violations, including everything from wrongful arrest, extending jailtime, and inappropriately registering people to the sex offenders list. While all software can face bugs or security flaws, or improper configuration, the errors resulting from this transition were very serious, including deploying the police against innocent people, often in ways that had significant impacts on their lives. The court issued statements acknowledging that mistakes had been made but continued to use the system. **A contract structured differently might have allowed them to compel the vendor to fix the problem, and could have prevented the delay in solving this issue caused by disagreement over vendor/court obligations.** Here, the point is that the typical response to a 'software bug' and the typical response to improper use of police power are extremely different, so when courts procure and use software that has the potential to impact peoples' freedoms, they should take great care in the contracting.

Warranties, Guarantees, and Representations

One of the major differences between analog and digital contracts is that analog contracts make a lot of affirmative promises – especially about the fitness of a product for a specific use. Not so with digital contracts. Yet, without those promises, courts are often left without the tools to make informed decisions about how to reasonably rely on digital services, and court stakeholders are left without a clear roadmap for who is responsible for answering inevitable questions and resolving disputes.

New Case Management Software, Part 2: One of the most jarring aspects of the above example is how complicated it was for the parties involved, all of whom just wanted working case management software that produced correct outcomes, to agree on a process for resolving the problem. Some of the first people to notice the problem were public defenders, who ultimately filed more than 2,000 declarations related to errors arising from this issue – and who courts eventually ruled didn't have the standing to challenge court-procured software, 'in their own right'. Clerks from an additional 3 counties also filed suit, as did a victim of wrongful arrest, none of which are, of course, an appropriate way for courts to identify, resolve, or redress the harms caused by a software system. When negotiating technology contracts, whether commercial or custom, they should assume that significant updates – whether because of flaws, as in this case, or because of updated policy, as in the Arizona case – will be required and budget accordingly. **Ensuring a court's procedural rights by assigning responsibility for software updates, maintenance, and adaptation is a key component of effective technology procurement and contracting.**

Building for Iteration, Interpretation, and Adaptation

Court services are themselves designed to adapt – typically because of the participation of their stakeholders. Digitally transforming court services increases the potential to continuously improve service delivery, but it also requires proactively providing and contracting for systems that articulate the process for making those improvements. And, as described in the NCSC's Principles for Post-Pandemic Court Technologies, the most effective systems enable court stakeholders to participate in designing those improvements. Courts' digital services contracts should include provisions that permit the court to continuously improve the product over time to adapt to the needs of litigants or statutory or rule changes.

Always Build an Off-Ramp

History has shown us that it is likely that some digital services or companies will fail, so courts need to design digital transformation processes with succession in-mind from the beginning. NCSC has created a resource designed to help courts do just that, which is available here.[5] This approach is not only important for long-term planning, but is also useful to help courts avoid vendor lock-in – which is especially common in digital services. Courts' digital services contracts should include wind-down provisions that not only give them a copy of the underlying data, but also enable them to transition to another system without losing continuity of service. Courts should approach digital transformation with clearly articulated provisions that provide for redundancy, resilience, and succession in service provision.

Getting (and Losing) Your Fibre: Building off-ramps is important for all kinds of technology procurement – including infrastructure services. In 2019, just two years after Google Fiber began signing subscribers in Louisville, Kentucky, the company decided to cease local operations. They gave customers two months of notice and free service, before shuttering. While switching Internet providers is relatively solvable, switching software and service providers can have big impacts. **The more courts contract technologies with succession as an assumption, the more independent and resilient they are when the unexpected, inevitably, happens.**

[5] Linked above at www.ncsc.org/exitingtech this resource was developed in partnership with small scale. You can use the link to access an online version of the tool or request a free booklet. You can also watch a short video overview of the tool here.

Contracting Digital Fairness, Fairly

Courts' rapid engagement in digital transformation creates an often-overlooked source of influence: public purchasing power. Courts, by engaging in digital transformation, are also creating an opportunity in which they can wield their resources, individually and collectively, to shape the market for the digital services they use. However, for courts to capitalize on that opportunity, they need to be able to express the principles above – not just as concepts but translated into the contractual terms that formalize their underlying rights.

To help courts translate the principles above into usable practice, this white paper highlights key provisions in two common types of digital contracts: (1) digital work-for-hire contracts and (2) platform terms of service. Each of these contracts represents a different approach to managing digital services infrastructure and, as a result, a different kind of relationship. Work-for-hire contracts, for example, are where a court hires a contractor to build, customize, or license a product. By contrast, terms of service agreements are most common in relationships where a court uses commercial, off-the-shelf platform services. These contracts are different from each other because they represent different kinds of relationships between a digital service provider and a court, and those differences have an impact on the resulting needs and power dynamic of each party. In some cases, those differences may prevent the parties from negotiating at all.

Courts can create a unique role and support infrastructure for their digital services, but doing so will require them to assert firm standards for their procedural rights in the relevant contracts. The way that courts design and deliver digital services will inevitably change over time, so the first step in building fair digital services is to ensure that the underlying contracts preserve courts' ability to drive those changes fairly.

Work-for-Hire Digital Services Contract

Typically, work-for-hire digital contracts are used to hire technical talent for short periods to set-up digital services systems. The key priority for courts using work-for-hire contracts for digital services should be ensuring that they have access to the legal authorities and technical resources necessary to independently sustain the procured system beyond the term of the agreement.

Here are a few key provisions to pay attention to in work-for-hire contracts:

Intellectual Property clauses are often used to create dependence on a digital service provider. Courts should ensure that they have a broad license to use, alter, and create derivative products from the outputs of the agreement – essentially, courts need to make sure that vendors cannot assert intellectual property rights to limit courts' use of the underlying technology.

Courts can also require vendors to guarantee that their work product does not have any third-party interests, dependencies, or licenses that require court attention. This does not

mean that courts need a proprietary license to the intellectual property embedded in their digital systems – open licenses, non-commercial licenses, and software collaboratives all offer creative solutions to protecting courts' interests without infringing on the interests of the vendor.

Confidentiality clauses in digital contracts often extend to protect technical development processes as trade secret, which can significantly limit a court's ability to maintain or adapt the procured technology. Here, it is most important for courts to ensure that confidentiality clauses are not used to foreclose ongoing use of, or migration away from, procured digital systems.

The Scope of Work may seem obvious, but it is easy for digital work-for-hire contracts to fall prey to ambiguities. All technology products are imperfect, so when courts hire a vendor to build a system, they often assume that the product will reach an obviously 'final' state, which will mark the end of the contract.

Unfortunately, this may not happen – it is far more common to realize, once a court has established some basic functionality, how more refinement and support could help the court achieve additional goals. The same is true for product customization and maintenance work, whether the court is contracting website design, software development, or something even more complex. In digital contracting, the term 'acceptance criteria' is used to establish the functional and contextual requirements that enable both parties to consider work complete. Critically, these acceptance criteria need not only to describe the technical functionality required but also the conditions under which a product should achieve that functionality. For courts, that means articulating specific acceptance criteria to ensure that contracted products realize their intended purpose.

Terms of Service Agreements

Terms of service agreements are how commercial, off-the-shelf platforms govern their relationship with their clients. Unlike work-for-hire contracts, terms of service are usually boilerplate contracts that use a common set of terms to govern their relationship with all users, regardless of the type of user or technology use. As a result, platform companies often confer broad authorities to themselves in terms of service agreements, including the ability to unilaterally amend the agreement. Similarly, terms of service typically focus on technical functionality, as opposed to the fitness of that functionality for specific uses, or the liabilities that might reasonably arise from those uses. In addition, terms of service agreements often frame digital rights in commercial terms, which can flatten or exclude other rights protections available to courts and their stakeholders. The asymmetry in these agreements can present a challenge for courts expecting specialized attention or customization to meet specific needs.

Courts are best served by viewing commercial digital service providers as an extension of their organization and as an assignment of their public authority. Courts entrust digital service providers to perform critical aspects of their relationship with court users, often in

ways that impact the equity of the service – everything from ensuring the accessibility of public resources to presenting unbiased research to protecting sensitive information. **As a result, a court's key priority in negotiating terms of service agreements should be ensuring the ability to establish, maintain, and enforce standards of transparency, equity, and accountability.**

Here are a few key things to evaluate in terms of service agreements:

Data License: Terms of service agreements frame platforms' use of data as necessary to provide their services – including the types of data they collect, what they use it for, and who they share it with. As described above, though, these terms can be phrased quite broadly, both because services grow over time and because the companies that administer them change. Most companies reduce the amount of contract amendments necessary by using relatively broad categories as the bases of their data rights, expecting users to trust their internal systems to prevent abuse.

Courts should review terms of service with an eye toward understanding that platform's data rights and ensuring they are appropriate for court stakeholders, as well as courts themselves. For example, terms of service agreements often enable platforms to use the data they collect through service provision to perform analytics, conduct 'research', support the company's marketing, or share that data with subsidiary technology services. Each of these categories can be sensible, but they can also become the source of significant abuses of court stakeholders' basic rights and interests. Courts using technologies that generate, categorize, or publish data about stakeholders should include provisions that ensure both transparency and acceptable use limitations., Proactive contracting can ensure that courts do not become a source of data exploitation, as can be the case in a range of important public services.

Acceptable Use: The acceptable use section of a terms of service agreement is where a platform company describes what their users are allowed to do with the platform. Typically, terms of service frame acceptable use as "all legal uses," with a list of specific prohibitions against illegal, harassing, or otherwise inappropriate behavior. Importantly, platforms often also reserve the right to unilaterally interpret, adjudicate, and enforce those prohibitions. Courts' use of technology is unlikely to upset most 'acceptable use' policies, but they are important to understand – as courts may be held responsible for other court stakeholders' behavior, which can result in suspension or loss of access from a platform. Where courts should focus negotiating influence is on improving the accessibility, transparency, and due process that goes into a platform exerting their authorities in determining acceptable use.

Privacy Policies and Nested Agreements: Several platform companies create multiple policies that govern different aspects of their authority. This includes privacy policies – both for the original service and, potentially, for linked services. For courts, this means that important information about the ways that service providers use court stakeholder data may be scattered across multiple agreements or buried in an obscure link, deep in

the terms of service. Courts negotiating terms of service agreements should work toward specific, affirmative data use descriptions – with explicit limitations requiring additional agreement for uses that exceed those terms.

While these are a few areas to focus on in digital services contracts, they are only intended to illustrate the ways that contracting terms and tactics meaningfully shape the equities between parties. Of course, when courts are contracting for digital services, they are not just a commercial actor, they must consider the impact of these terms on the unique relationship they have to their stakeholders. Unlike digital platform users, like someone choosing to use Facebook, court users do not opt-in to their use of the service. A court user does not choose the court's case management system but ultimately must rely on it. They have not opted into the terms of service that govern the court's use of that system, yet they may end up having their rights governed by those same terms of service. The fact that someone is opting into use is a founding assumption of most contracts, which does not necessarily hold true for courts and their users. Beyond basic consent issues, courts need to be mindful of how data collected through the administration of services could be used by third-parties.

At an operational level, courts' transformation into digital actors not only means developing the capacity to engage with technology providers, it also means developing the mechanisms to articulate, monitor, and enforce the rights, limits, and conditions the court creates in digital contracts. While that can seem daunting initially, the process of designing and negotiating for data rights through contracting processes is the first step to building both sources of capacity, in addition to improving the efficiency and effectiveness of their services.

Conclusion

Digital transformation offers incredible opportunities to realize the promise of court services, in no small part because extending the reach of courts to equally serve a broader range of stakeholders is a foundational component of the promise of new technology. Courts are unique in a range of important ways – often in ways that can be altered or diminished by digital transformation unless they take care in how they contract and assign rights.

In the short-term, courts' recent, rapid digitization has resulted from incredible ingenuity in adapting to the extraordinary demands of pandemic response. However, public systems are only now starting to recognize the impacts of these changes. In the long-term, courts are best served by advocating as ardently for their unique needs as possible, not only because of self-interest, but because it creates models and markets that can serve other public institutions. Unfortunately, in today's digital markets, that may mean that courts need to work even harder to find less-obvious, more-aligned partners – but that investment in research, diligence, and procurement both returns capacity benefits and, importantly, helps build the foundations for the kinds of post-pandemic data and technology use envisioned in the principles bulleted above on the first page of this paper.

This white paper is intended to facilitate courts' ability to negotiate digital contracts in a way that, toward preserves their unique character and realizes the aspiration of fair, digital court services. If this guide raises questions, conversation, or an interest in further engagement, please reach out to the National Center for State Courts.

Suggested Citation:
Access to Justice Team. *Contracting Digital Services for Courts*. [Williamsburg, VA: National Center for State Courts, 2022]