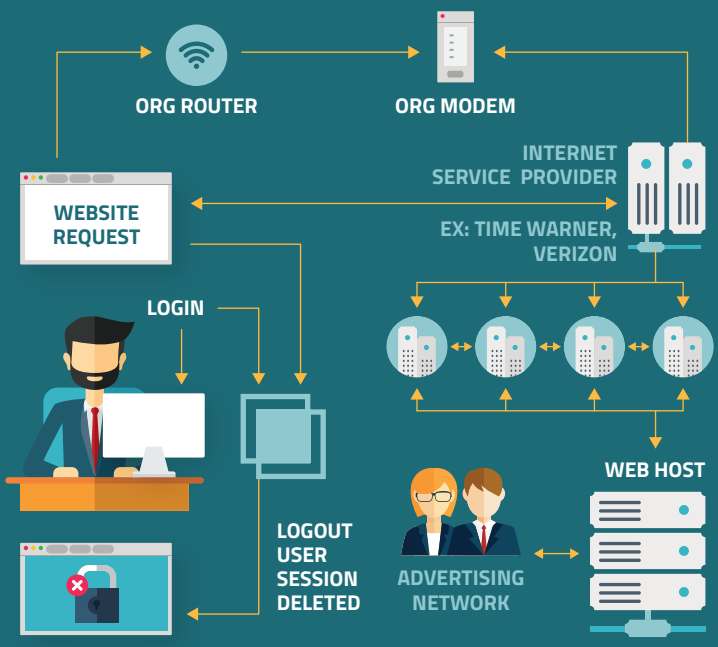
Don't let cybersecurity become the next digital divide!

THINGS CIVIL JUSTICE COMMUNITY CAN DO NOW!

- **Map data flows,** to provide a high level view of the flow of information, where data comes from, where it goes and how it gets stored in your office.



- **Develop a privacy, cybersecurity, and data-sharing plan** vetted by security experts. Cybersecurity threat assessments should look at both the organization and the end-users/clients.
- **Explore alternative web analytics programs,** like Piwik.org which gives you 100% data ownership – as opposed to Google/Universal Analytics which use your data for business purposes.
- **Know what data discrimination is,** as well as what disparate impact on data mining is, particularly when developing technologies which rely on algorithmic and/or data-driven decision-making (i.e. expert systems, litigant portals, etc).
- **Know the risks your clients face when using A2J technologies and mobile phones,** when developing new technologies, outline the privacy and security implications that arise when lower-income individuals increasingly have to use tech and mobile-enabled tools for accessing justice.
- **Know what mobile phones & tablets your clients use:** Start collecting information on the technology your clients use, especially mobile phones. For example, clients who can only buy the cheapest possible smartphone may be most at risk to surveillance and mobile security issues such as mobile malware.
- **Ensure your staff know how to share documents and data securely,** two recommended tools are: IronBox and Box.
- **Train your staff on best practices for using their devices for work,** make sure to outline security considerations and implications and they are aware of key tools such as: Eraser (for HHD) as well as SSD Toolbox and Samsung Magician Software (for SSD).
- **When collecting data first hand, always think through security practices,** for example use this website: EncryptAllTheThings.net – for a list of top-level things to think through when protecting databases.
- **Familiarize with key frameworks** for cybersecurity and privacy: Such as: Privacy Risk Management for Federal Information Systems and Framework for Improving Critical Infrastructure Cybersecurity.
- **When contracting with third-parties watch their terms, and follow up to know how serious they are taking security,** this is a useful case to consider: Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk

ACLU AMERICAN CIVIL LIBERTIES UNION · accessnow · Data&Society RESEARCH INSTITUTE · FLORIDAJUSTICE TECHNOLOGYCENTER coordination | collaboration | innovation · JUST TECH