epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

Introduction and EPIC's Cy Pres Qualifications

The Electronic Privacy Information Center (EPIC) is a 501(c)(3) nonprofit public interest research and advocacy center in Washington, D.C. Our mission is to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and education. Our work is cited and relied upon by policymakers, scholars, and privacy professionals around the world. We have long advocated for robust privacy protections at the federal and state level. We have written extensively on consumer privacy issues under the Telephone Consumer Protection Act, the Electronic Communications Privacy Act, the Video Privacy Protection Act, California Invasion of Privacy Act, California Consumer Privacy Act, the Federal Trade Commission Act, and many other privacy laws.

EPIC satisfies the two key requirements for being a recipient of *cy pres* funds in a consumer privacy, data breach, robocall, web tracking, biometric privacy, health privacy or wiretap case: EPIC is both aligned with the interests of class members and advances the aims of the underlying litigation. EPIC has also had a strict independence policy since its inception and does not accept donations or sponsorships from corporations or government entities. This sets EPIC apart from many other organizations and ensures that our position is always based solely on the public interest. Moreover, funds directed to EPIC are sure to serve the interests of class members in privacy and web tracking cases. EPIC directs 83% of revenue to program activities—a top-tier standard for non-profit management.

Courts have approved EPIC as a *cy pres* recipient in numerous consumer privacy cases, including *Mirfasihi v. Fleet Mortgage Corp.*, 03-1069 (N.D. Ill.); *Perkins v. LinkedIn Co.*, No. 13- 4303 (N.D. Cal.); *In re: Vizio, Inc. Consumer Privacy Litigation*, 8:16-ml-2693 (C.D. Cal.) (SCA & Wiretap Act); *Abramson v. American Advisors Group, Inc.*, 19-cv-1341 (W. D. Pa.) (TCPA); *Dolemba v. Champion Roofing*, LLC, 19-cv-7139 (N.D. Ill.) (TCPA); *William Harrison v. The Irvine Company LLC*, 30-2018-00978745 (Orange Cty. Sup. Ct.) (FACTA & FCRA); *Lopez v. Superior Health Linens, LLC*, 19-cv-02390 (N.D. Ill.) (BIPA); *In re Google Plus Profile Litigation*, 18-6164 (N.D. Cal.) (data breach); *In re: Google Street View*, 10-2184 (N.D. Cal.) (Wiretap Act); *Krakauer v. Dish*, 1:14-cv-333 (M.D.N.C.) (TCPA); *In re: Netflix Privacy Litigation*, 5:11-CV-00379 (VPPA); *Lane v. Facebook*, 10–16380, 10–16398 (Wiretap Act, VPPA); and *In re: Lenovo Adware Litigation*, 15-md-02624-HSG (N.D. Cal.) (CFAA & CIPA).

In *Perkins v. LinkedIn Co.*, the court found that EPIC is a "well-established and respected organization within the field of internet privacy" and is thus "well-suited to be a *cy pres* recipient." In *Mirfasihi v. Fleet Mortgage Corp.*, the court found that a *cy pres* distribution to EPIC "did cause an improvement in the settlement that provides additional benefits to the plaintiffs and to the community."

EPIC's Programs and Projects

- **Consumer Privacy**: EPIC's Consumer Privacy and Data Protection program seeks to reshape the legal and regulatory landscape in the U.S. to establish meaningful limits on both the collection and use of personal data. Under this program, EPIC challenges commercial surveillance by advocating for data minimization principles that ensure our digital systems are designed to empower and protect users while fostering innovation. EPIC is a leading advocate for strong privacy protections at both the state and federal level.
- **Data Protection and Cybersecurity**: The security of data, computer systems, and critical infrastructure is essential to the functioning of our society. EPIC supports improved cybersecurity standards and oversight to protect against breaches and to ensure a quick and robust response when they occur. We know that while the continued innovation of computer systems and networks has brought many benefits, it has also opened the door to significant cybersecurity risks. Both private sector and government systems are subject to attack, and breaches of systems can have severe consequences, especially when records include sensitive financial and health information.
- **Robocalls and Communications Privacy**: EPIC has extensive expertise in defending the privacy of telephone subscribers from the persistent threats of robocalls, scams, and security breaches. This includes supporting vigorous enforcement of the TCPA prohibition on unwanted automated calls and texts; advocating for limits on the collection and use of telephone numbers and other subscriber data; researching and educating the public about robocalls and subscriber profiling; and advocating for greater restrictions on the collection and sale of subscribers' personal information for unwanted telemarketing and other purposes.
- **Health Privacy**: In recent years EPIC has focused increasing attention on the protection of personal health data. We have called on agencies including the Federal Trade Commission, the Consumer Financial Protection Bureau, and the Department of Health and Human Services to strengthen health privacy protections through rules, guidance, and enforcement. Addressing emerging privacy threats to health information in the digital ecosystem is crucial, and now is the moment to explore solutions that can advance individual protections and promote greater health equity.
- **Web Tracking, Wiretapping, and Social Media Privacy**: EPIC has raised concerns about the growing use of advanced tracking techniques (such as Pixel tracking) that allow companies to track users as they browse the web, gaining troves of personal information on individuals that can be used to develop behavioral profiles for targeted advertising. EPIC has done extensive work in the areas of online tracking and behavioral profiling, including urging the FTC to limit the use of cross-device tracking, whereby companies track consumers across their smartphones, laptops, tablets, and other internet-connected devices. Social media companies—and in particular, Facebook—collect vast quantities of personal data in order to "microtarget" advertisements to users. This practice, also known as surveillance advertising or behavioral advertising, is deeply harmful to privacy, the flow of information, and the psychological health of social media users. For more than a decade, EPIC has advocated before Congress, the courts, and the Federal Trade Commission to protect the privacy of social media users. EPIC has also

advocated for a number of changes to ECPA including an across-the-board warrant requirement, search notice and returns for users, protection of location data, and mandatory data minimization and end-to-end encryption for commercial e-mail services.

- **Biometrics and Facial Surveillance**: EPIC advocates for meaningful safeguards on personal data collection and processing to ensure that individuals are protected from abuse, exploitation, discrimination, and invasive surveillance. Because improper collection of this information can contribute to identity theft, inaccurate identifications, and infringement on constitutional rights—and because biometric identifiers cannot be changed—EPIC advocates for heightened protections for biometric data. Illinois' BIPA is one of the strongest and most effective privacy laws in the United States; to that end, EPIC has urged other states to pass similar bills protecting biometric information.
- **AI and Human Rights:** The deployment of artificial intelligence and automated decision-making systems has exploded in recent years across both the public and private sectors. Not only are these systems used to make life-altering decisions, but they are also often deployed in opaque ways that can exacerbate biases and harm individuals. EPIC advocates for transparent, equitable, and commonsense AI policy and regulations. EPIC focuses on AI procurement, AI policy, and commercial AI use, among other topics.
- **Platform Accountability and Governance**: Online platforms increasingly permeate our lives. We use them to find and read the news, to buy goods, to find and book travel, to date, to find a place to live, and more. EPIC advocates for platform governance and accountability policies that protect the speech, privacy, civil rights, and safety of internet users. EPIC works to ensure that platforms are held accountable for violating the law by advocating for reasonable interpretations of the First Amendment, Section 230, and Article III standing doctrine. EPIC's Platform Governance and Accountability team coordinates and files amicus briefs in key cases, provides support to litigators, consults with lawmakers, and engages with regulators.

How EPIC Allocates *Cy Pres* Funds

- Developing educational materials on privacy and data protection such as informational blog posts, fact sheets, newsletters, and privacy law explainers.
- Providing expertise to lawmakers through technical assistance and testimony.
- Publishing reports that seek to educate the public, lawmakers, and regulators about emerging privacy and technology issues. Some examples include: *Generating Harms I & II: Generative AI's Impact & Paths Forward, The State of Privacy: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better, and Scam Robocalls: Telecom Providers Profit.*
- Submitting comments, letters, and complaints to federal and state agencies urging them to strengthen privacy regulations and enforcement mechanisms.
- Filing "friend of the court" briefs to reinforce the legal obligations of government agencies and businesses to safeguard personal data.
- Coordinating coalitions and groups to collaborate on larger projects and initiatives.

EPIC is well situated to use funds to stand up new initiatives or projects. For example, EPIC created a Telephone Subscriber Privacy Project with the support of a *cy pres* award in *Krakauer v. Dish Network*. EPIC works on the federal and state level and is equipped to undertake state-specific work. For example, EPIC has a project focused in California funded by *cy pres* funds granted through the Rose Foundation for Communities and the Environment.