

**NEW YORK STATE BAR ASSOCIATION
HOUSE OF DELEGATES
RESOLUTION ADOPTED APRIL 4, 2009**

WHEREAS, the mission of the Privacy Task Force was to: (1) identify discrete areas of privacy for lawyers and those they represent (businesses and individuals) concerning the Internet, health and financial information; (2) review the laws, statutes and rules in these areas; (3) propose procedural and substantive changes where necessary; (4) provide opportunities to educate the profession and the public on privacy with the aim of ensuring that our laws, policies and practices are designed to reduce the risk of violations of privacy; (5) review and report on the current remedies/compensation available to those whose data have been seized for illegitimate purposes; and (6) prepare a report which covers the current state of the law and shall recommend any appropriate reforms, both by statute, policy and practice, to the Executive Committee and the House of Delegates; and

WHEREAS, the Privacy Task Force fulfilled its mission and prepared such report, inviting input from all Sections as well as from specialty, local, and county bar associations and privacy experts; and

WHEREAS, the Privacy Task Force held a Privacy Summit in New York City where experts in privacy law identified some of the most pressing areas in privacy law at this time; and

NOW, THEREFORE, IT IS

RESOLVED, that the New York State Bar Association approves, with its thanks, the Report of the Privacy Task Force; and it is further

RESOLVED, that the Association endorses certain best practices set forth in the Report: (1) that web site owners should include the provisions on pages 40-43 of the Report in their Terms of Use; (2) that web site owners should include the provisions on pages 46-47 of the Report in their Privacy Policy; (3) that lawyers should take steps to avoid or mitigate the risk that client information obtained in the course of their legal practice, the privacy of which is protected by federal, state or local law, will be accessible to unauthorized persons (see pages 49-60); (4) that lawyers should treat health information obtained in the course of their legal practice with the appropriate standard of care to meet the privacy protections required by applicable law (see pages 77-125); (5) that lawyers should take reasonable steps to protect medical records and other health information obtained in the course of their legal practice from destruction or inadvertent disclosure, theft or other security breach (see pages 102-106); (6) that discovery request respondents should seek to address reasonable privacy concerns in responding to discovery requests (see pages 209-221); and (7) that agencies should strive to commit adequate resources to enforce compliance with existing privacy laws; and it is further

RESOLVED, that the Association reaffirms its commitment to the goal of providing opportunities to educate the profession and the public on privacy and suggests interdisciplinary

CLE programs be conducted to address the following areas identified by the Task Force and experts in privacy law as some of the most pressing areas in privacy law at this time:

1. Medical Information Technology: (a) agency and government enforcement of privacy regulations for compliance and funding to permit smaller organizations to become compliant without oppressive financial cost; (b) the effectiveness and enforcement of penalties for poor or breached security; (c) assistance to covered entities to implement internal controls, including education of medical personnel to ensure proper, secure, and compliant use of information systems; (d) whether there should be private rights of action for breaches of medical security; (e) whether patients should be able to opt-out of having their records in a national healthcare database and the implications of such; and (f) whether information voluntarily submitted to medical databases (e.g., Google Health) should be subject to new privacy protections and regulations that arise out of the recently enacted stimulus legislation.
2. Employment: The extent to which an employer may access and use information (both employment and non-employment related) about an employee or potential hire, including information about the individual posted on the Internet that cannot be readily verified and material posted on social networking sites.
3. Record Retention and Destruction: The disposal, destruction, and maintenance of client files (both paper and electronic) by lawyers and law firms, including whether there should be a “catch-all” period for mandatory destruction of all records containing non-public personal information of consumers;
4. Bankruptcy Issues: The ability and preconditions to sell private consumer information in bankruptcy proceedings as an asset of the bankruptcy estate (for example, when a privacy notice says that the bankrupt company doesn't share information);
5. Social Security Numbers: The use of Social Security numbers as an identifier for any purpose, with a specific focus on: (a) how to prevent future use of Social Security Numbers as common identifiers; (b) how to remedy past and present abuses; (c) what is an appropriate alternative for authenticating identity (e.g., biometric identity cards);
6. Uniformity in Breach Notification Laws: Whether there should be a national standard for data breach notification;
7. Enforcement and prosecution: How to enforce and prosecute data breaches and privacy violations such that the risk of inadequate data security and privacy violations are more than merely a “cost of doing business”; and
8. Technology Standards: Whether a baseline can be established as to the minimum level of technological protection an attorney must use in protecting client information and the attorney-client privilege;

and it is further

RESOLVED, that the officers of the Association are hereby empowered to take such other and further steps as they may deem warranted in order to implement this Resolution.