The Law and the Internet for IAFF Affiliates

International Association of Fire Fighters
Legal Department
1750 New York Ave NW
Washington, DC 20006
(202) 737-8484

Special thanks to the IAFF Information Technology Department and local officers for their edits and ideas for this manual.

TABLE OF CONTENTS

Electronic or Online Voting

For the computer-savvy IAFF leader and member, online balloting might seem like an easy way to simplify IAFF affiliate elections and union referenda, and for some kinds of voting, that might be right. But for all IAFF locals, certain types of elections cannot be conducted using online balloting, and for a small group of IAFF locals (I-locals and F-locals, mostly), there are additional restrictions.

For many locals conducting votes (such as contract votes), elections for officers that do not – by virtue of their office – become delegates to the convention, and special elections, online balloting is a lawful and cost-saving approach. It may be done, so long as it is permitted under a local's own constitution and by-laws. In addition, a local must confirm that online voting is permissible under state laws. At this point, IAFF affiliates' experimentation with online voting is just starting. The IAFF will be reviewing locals' practices and experiences and will attempt to develop some best practices. It is advisable, however, that locals interested in conducting online voting ensure that the service provider can also allow non-computer savvy members to vote, even without a computer, using an alternative method like telephone voting. Many service providers do make this available as part of an online voting system.

Please note that online *polling* (i.e., just getting a sense of what members want, without any force of law) is not prohibited. In fact, it can be a good way to measure support or opposition prior to a vote.

I. Frequently Asked Questions

Can An Affiliate Use Online Voting for Elections?

Online voting does **not** comply with the federal "secret ballot" requirements that pertain to officer elections, and sometimes, certain union referendum votes. So, where a given election is covered by federal law, it cannot be done by online voting.

There are a number of situations where IAFF affiliates are required to conduct votes in compliance with federal law. For instance, federal regulations require that secret ballots be cast in elections for delegates to the IAFF Convention, including the election of union officers who also serve as IAFF Convention delegates by virtue of their office. The term "secret ballot" is defined by the federal government in a way that makes online voting, right now, non-compliant.

Federal regulations define "secret ballot" as meaning "the expression by ballot, voting machine or otherwise… of a choice… cast in such a manner that the person expressing such choice cannot be identified with the choice expressed." While this federal law, in most respects, does not apply to many IAFF affiliates, the law does apply to the IAFF itself, and therefore to the election of delegates to the IAFF Convention – even for public employees or members in Canada.

Most online voting systems available today that advertise the ability to run "secret ballot elections" utilize an electronic balloting system that allows a third-party administrator unconnected with the union to identify a ballot with the voter. For this reason, it does not technically satisfy the federal "secret ballot" requirement.

If certain officers of a local are automatically delegates to the IAFF Convention, the elections for these offices – if the winner is expected to attend the IAFF Convention – must be conducted in accordance with the definition of "secret ballot" under federal law. Therefore, any office that is automatically a delegate to the IAFF Convention cannot be elected by online vote. Conversely, any office that is *not* (by virtue of office) a delegate to the IAFF Convention may be elected by online vote, so long as the online vote is carried in accordance with the criteria below. (See "Online Voting Criteria," below.)

Can An Affiliate Use E-mail for Elections Notice?

In elections for officers who are delegates to the Convention, federal law also requires that membership be notified of the time, date, and place of the election via U.S. Mail. For that reason, while an *e-mailed* notice to members about the time, date, and place of the election is not prohibited, it is still not sufficient to comply with current law for the election of delegates. If your local is conducting a ballot-box vote for officers who, by virtue of office, will serve as delegates to the IAFF Convention, then the notice of the time, date, and place of the election must be sent either in a separate mailing, or alongside any other separate mailing (such as the local's newsletter). It cannot be sent by e-mail alone.

Can An Affiliate Use Online Voting For Dues or Assessment Increases?

While U.S. law also has requirements for locals to conduct votes on increases in initiation fees, reinstatement fees, dues, or assessments, locals that represent only public (non-federal) employees and locals in Canada need not comply with U.S. law on dues or assessment votes. Thus, online balloting for those particular locals (we call them "non-LMRDA locals") on increases in initiation fees, reinstatement fees, dues, or assessments is not prohibited, as long as the balloting meets the Online Voting Criteria below.

IAFF locals are required by Article XIII, Section 4 of the IAFF Constitution to conduct "secret ballot" referenda to approve proposed increases in initiation fees, reinstatement fees, dues or assessments. However, the General President has not defined "secret ballot" under the IAFF Constitution exactly to the same criteria as found in U.S. law. That is addressed in the next section.

The general rule is as follows for dues and assessment increases: if the affiliate represents any private-sector or federal employees, votes on dues increases or assessments cannot be conducted by online vote. If the affiliate does not represent any private-sector or federal employees (for example, it only represents municipal fire fighters), then the vote may be conducted online so long as it meets the Online Voting Criteria below.

II. Online Voting Criteria

The IAFF's own Constitution and By-Laws requires certain votes (officer elections, dues assessments, etc.) be conducted by "secret ballot." This is the same term as used in the federal law, but where the federal law does not apply, the General President has employed a slightly different interpretation of the term. Therefore, to meet the "secret ballot" definition for certain votes (for example, increases to dues for non-LMRDA locals, or election of officers who will *not* be delegates to the IAFF Convention), an online voting system would have to meet, at minimum, these criteria:

- guarantee secrecy;
- ensure a proper and accurate vote count;
- authenticate the eligibility of each voter;
- safeguard against potential hackers;
- limit a member to one vote cast;
- protect against computer viruses;
- make the Internet or e-mail accessible to its members;
- protect against the interception or alteration of votes;
- instruct members on how to vote electronically;
- ensure that the web server does not crash during the voting period; and
- ensure that a process is available to conduct a recount of the ballots if necessary.

Several online service providers advertise the ability to conduct online elections for locals. We strongly suggest that any online elections be conducted by a reputable service provider with no formal or informal connection to any local leader or board member.

If affiliate leaders have questions about selecting a vendor to provide online voting services that meet these criteria, they may contact (though their District Vice President) the IAFF's Information & Technology Division for assistance.

The IAFF is aware that the National Mediation Board and National Labor Relations Board have adopted "Electronic Voting" that enables election participants to cast their votes through a telephone and an online system. However, those votes are conducted under the Railway Labor Act, which does not apply to IAFF affiliates.

III. Revising a Local's Constitution and By-Laws to Allow for Permissible Online Voting

Affiliates that amend their constitution and by-laws to allow for electronic balloting *must submit their amended constitution and by-laws to the IAFF General President for approval, pursuant to Article XIII, Section 3 of the IAFF Constitution,* following the amendment's adoption by the local union. The General President's office will review any such amendments with the above-referenced concerns in mind.

If an affiliate is considering moving to an online system, here are some approved sample provisions from local constitution and by-laws:

> *Sample 1: Electronic Balloting Procedures - The ballot will be prepared and reviewed by the Election Committee prior to being posted on the web site to each member in good standing of Local #__, at least 15 days prior to the election. The vote will be conducted by a secret ballot electronically over the Internet. A date will be selected by the committee as to when the election will open and close. During the election period no access to the administration area (Online Voting) on the web site will be allowed by the E-Board or members. The only access to the administration area (Online Voting) will be given to the election committee and that access is to validate the vote only. If a problem arises, the Webmaster will inform our election committee of the problem and the election committee will determine how to proceed with instructions to the membership. After the election has been completed by the announced date, a copy of the results will be provided by our webmaster to the Election Committee. The Election Committee will confirm with the webmaster that no member has accessed the administration area (Online Voting) during the election.*
>
> *Sample 2: Electronic/On-line voting may be used for the election of officers who are not to serve as delegates to the IAFF Biennial Convention, or for any issue submitted to the entire membership for a vote. The computer program shall, at a minimum, contain the following elements: (1) sufficient encryption to ensure security and authenticity of the vote; (2) a mechanism to ensure each a member votes only once on each issue and that the member's identity is secret; (3) password protection, and; (4) the ability to calculate total votes. Online voting shall be available on the Internet, and only accessible to members of the Local.*
>
> *Except for elections for officers as described above, a matter may be submitted for consideration by the membership via electronic/on-line voting only where confirmed by the Executive Board.*

If an affiliate adds language on electronic balloting to its constitution & by-laws and that language is reviewed and approved by the General President's office, the final, updated version of the local's constitution & by-laws should be submitted to the IAFF in a searchable electronic format (MS Word, Rich Text, Plain Text computer file) in accordance with Resolution 7, which was approved by the delegates at the 2010 IAFF Convention.

The Internet and the First Amendment

The First Amendment provides substantial rights to locals and their members when using the Internet as a forum for speech. Nevertheless, locals and members must exercise great caution when posting information online.

The First Amendment prohibits Congress from passing a law that would restrict an individual's freedom of speech. The First Amendment is applicable to the states through the due process clause of the Fourteenth Amendment. When the state acts as an employer, rather than as a sovereign, the courts have recognized that the employer possesses a limited interest in regulating the speech of its employees.[1]

In *Connick v. Myers*, the Supreme Court indicated that it had "[o]ne hundred years ago… noted the government's legitimate purpose in 'promot[ing] efficiency and integrity in the discharge of official duties, and [in] maintain[ing] proper discipline in the public service."[2] The Court has recognized that, "when someone who is paid a salary so that she will contribute to an agency's effective operation begins to do or say things that detract from the agency's effective operation, the government employer must have some power to restrain her."[3] In other words, a public employer can discipline an employee for his or her speech or behavior both on and off the job.

This does not mean, however, that a public employee is without First Amendment protection. Rather, the Court has developed a two step "balancing" test to determine whether an employee's speech is protected.[4] First, the court asks "whether the employee's speech as a citizen was on a matter of public concern."[5] If the answer to that question is no, there is no possibility for a First Amendment claim based on the employer's reaction to the speech.[6] If the answer is yes, the court then asks "whether the employer has shown that the employee's interest in expressing himself on that matter is outweighed by injury the speech could cause to the employer's operations."[7]

In determining whether the speech involves a matter of public concern, the court will look to the content, context, and form of the employee's speech, viewing it in light of the record as a whole.[8] For instance, the court in *Stroman v. Colleton County School District* held that "personal grievances or expressions about other matters of personal interest do not constitute speech about

---

[1] *See Pickering v. Bd. of Educ.*, 391 U.S. 563, 568 (1968) (holding that a public school teacher did not relinquish all First Amendment rights simply by accepting a public position, so the teacher should be allowed to comment on matters of public concern).
[2] *Connick v. Myers*, 461 U.S. 138, 150-51 (1983) (quoting *Ex parte Curtis*, 106 U.S. 371, 373 (1882)).
[3] *Waters v. Churchill*, 511 U.S. 661, 665 (1994).
[4] *Pickering*, 391 U.S. at 568.
[5] *Piscottano v. Murphy*, 511 F.3d 247, 270 (2d Cir. 2007). *Compare Garcetti v. Ceballos*, 547 U.S. 410, 421 (2006) (holding that employees speaking and acting within the scope of their employment, rather than as citizens, have no First Amendment claim and cannot use that as a shield against being disciplined by the employer).
[6] *Garcetti*, 547 U.S. at 418.
[7] *Piscottano*, 511 F.3d at 270.
[8] *Lilienthal v. City of Suffolk*, 275 F. Supp. 2d 684, 691 (E.D. Va 2003).

matters of public concern that are protected by the First Amendment."[9] Therefore, this type of speech would be subject to discipline by a public employer. In contrast, in *Lilienthal v. City of Suffolk*, the court determined that a fire fighter's repeated statements to members of the City Council regarding the safety, equipment, staffing, and response times of the fire department were matters of public concern that are protected by the First Amendment.[10]

In determining whether the employee's interest in free speech outweighs the injury that could come to the employer as a result of the speech, courts look to when and where the speech was made, and the likelihood that it will have a disruptive impact on the employer's working environment. For instance, in *City of Kokomo v. Kern*, a fire fighter was demoted after he made comments implying that his department had an ulterior motive for denying his fireworks display application. The court held that the demotion did not violate the First Amendment because the comments had the potential to disrupt the department, which requires discipline to function efficiently and effectively.[11] Similarly, in *Curran v. Cousins*, a police officer was terminated after he posted allegations on the union's web site that his department's correctional officers were discharged for supporting the sheriff's opponent in an election. Although the court recognized that a portion of the postings involved a matter of public concern,[12] the court found that the manner in which the allegations were made, by comparing the sheriff to Hitler and those who support him to Nazis, was likely to disrupt the operation and efficiency of the department.[13] Therefore, the court held that the department's interest in maintaining order within the department outweighed the officer's interest in free speech, and upheld his termination.[14]

In addition, even if an employee is speaking on a matter of public concern, he or she may still be disciplined if the speech is made in the employee's official capacity, and not as a citizen. In *Garcetti v. Ceballos*, the Supreme Court held that when "public employees make statements pursuant to their official duties, the employees are not speaking as citizens for First Amendment purposes, and the Constitution does not insulate their communications from employer discipline."[15] However, it declined to articulate a formula for determining when a government employee speaks pursuant to his or her official duties. While this has caused some inconsistency in the application of the First Amendment to public employees, most courts have limited First Amendment protection for any speech that is made in furtherance of his or her responsibilities, even if it is not expressly designated as part of his or her job duties.[16]

---

[9] *Stroman v. Colleton County Sch. Dist.*, 981 F.2d 152, 156 (4th Cir. 1993).
[10] *Lilienthal*, 275 F. Supp. 2d at 691.
[11] *City of Kokomo v. Kern*, 852 N.E.2d 623, 629 (Ind. App. 2006).
[12] *Curran v. Cousins*, 509 F.3d 36, 46 (1st Cir. 2007) (the lower court in *Curran v. Cousins*, 482 F. Supp. 2d 36 (D. Mass. 2007) noted that the fact that Curran expressed his views on the Internet was a factor in determining whether the matter was of public concern); *but see Garcetti*, 547 U.S. at 419 (holding that the fact that an employee confined his statements to the workplace was not dispositive of whether the statement was of public concern).
[13] *Id.* at 47-48.
[14] *Id.* at 49-50.
[15] *Garcetti v. Ceballos*, 547 U.S. 410, 421 (2006); *see also Valentino v. Village of S. Chicago Heights*, 575 F.3d 664, 671 (7th Cir. 2009).
[16] *See Weintraub v. Bd. of Educ. Of City Sch. Dist. of New York*, 593 F.3d 196, 203 (2d Cir. 2010) (holding that "under the First Amendment, speech can be 'pursuant to' a public employee's official job duties even though it is not required by, or included in, the employee's job description, or in response to a request by the employer");

For instance, in *Foley v. Randolph, Mass.*, a fire chief was disciplined after he addressed budgetary and staffing issues at a press conference following a fatal house fire. The fire chief argued that, because he addressed these issues as a citizen and not in his official capacity, his speech was protected by the First Amendment. The 1st Circuit determined that, even though the contract and statute governing the fire chief's employment neither required nor authorized him to speak to the press, "he had been in command of the scene, and when choosing to speak to the press, he would naturally be regarded as the public face of the Department when speaking about matters involving the Department." [17] Consequently, the Court held that "there was no doubt that… [he] was speaking in his official capacity and not as a citizen" and upheld his discipline.[18]

Finally, it is important to note that the First Amendment does not prohibit private employers from restricting their employee's free speech.[19] As the Fifth Circuit has stated, "while the employer has no right to control the employee's speech, he does have the right to conclude that the employee's exercise of his constitutional privileges has clearly over-balanced his usefulness and destroyed his value and so to discharge him."[20]

If a member believes that he or she is being unlawfully targeted based upon his or her speech, the local affiliate should immediately contact the IAFF Legal Department for assistance.

I. Frequently Asked Questions

Are locals responsible for the information that their members post on the local's web site or bulletin board?

Generally, locals, *as organizations*, cannot be held liable for the information their members post on the local's web site or bulletin board. As noted above, the First Amendment guarantees the right to freedom of the media and freedom of speech.[21] Recognizing that the ability to disseminate information is much greater through the Internet, Congress enacted the

---

Williams v. Dallas Indep. Sch. Dist., 480 F.3d 689, 693-94 (5th Cir. 2007) (holding that "[s]imply because [the employee] wrote memoranda, which were not demanded of him, does not mean he was not acting within the course of performing his job," and that "[a]ctivities undertaken in the course of performing one's job are activities pursuant to official duties"); *Renken v. Gregory*, 541 F.3d 769, 773 (7th Cir. 2008) (finding that when a professor who complained about the difficulty in administering an educational grant, he was speaking as an employee because the grant was "for the benefit of students" and "aided in the fulfillment of his teaching responsibilities," even though it was not a formal requirement of his job"); *Chavez-Rodriguez v. Santa Fe*, 596 F.3d 708, 714 (10th Cir. 2010) (*quoting Green v. Board of County Comm'rs*, 472 F.3d 794 (10th Cir. 2007) (holding that "'even if not explicitly required as part of her day-to-day job responsibilities,' an employee's statements are made pursuant to official duties when they 'stemmed from and were the type of activities that she was paid to do'")); *Phillips v. City of Dawsonville*, 499 F.3d 1239, 1242 (11th Cir. 2007) (finding that "a public employee's duties are not limited only to those tasks that are specifically designated").

[17] *Foley v. Randolph, Mass.*, 598 F.3d 1, 15 (1st Cir. 2010).

[18] *Id.*

[19] *Tiernan v. Charleston Area Med. Ctr., Inc.*, 506 S.E.2d 578, 589-91 (W. Va. 1998); *see also Hudgens v. NLRB*, 424 U.S. 507, 513 (1976) (holding that a constitutional provision guaranteeing free speech does not extend to private conduct).

[20] *Truly v. Madison Gen. Hosp.*, 673 F.2d 763, 767 (5th Cir. 1982).

[21] U.S. CONST. amend. I.

Communications Decency Act in 1996.[22] In enacting the CDA, Congress intended to encourage individuals and organizations to provide opportunities for others to freely share information and ideas online without fear that the provider would be subject to unfair litigation for the thoughts posted on their web site.[23] Therefore, Section 230 of the Act, known as the "Good Samaritan" clause, provides immunity to organizations that operate interactive web sites and bulletin boards from liability arising from the information that is posted on their web site or bulletin board by members or outside parties.[24]

In *Donato v. Moldow*, the court analyzed Section 230 as it applied to administrators of online bulletin boards. In this case, local government officials brought suit against the operator of an online bulletin board for posting messages that encouraged discussion of local government activities.[25] The officials alleged that the messages constituted defamation, harassment, and the intentional infliction of emotional distress.[26] Although the court assumed that some of the statements on the web site may have been actionable, they found that the operator of the web site could not be held liable because Section 230 granted him immunity.[27] The court was not persuaded by the official's argument that the operator should be held liable because he had previously deleted objectionable comments and posted retractions for statements he later learned were false. The court explained that the "Good Samaritan" clause protected web site operators, and would not impose liability for "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."[28]

Consequently, locals that wish to maintain web sites that allow others to post material to the site may do so without fear of liability, even if they manage the site in such a way that removes objectionable content. However, as discussed below, **individuals** (including web site administrators) who post objectionable content may be held liable under the Act as it is not intended to allow the Internet to be a place where people can speak without being held liable for speech that would otherwise give rise to civil or criminal liability were it spoken or published in traditional written format.

---

[22] 47 U.S.C. § 230(a)(1) ("The Congress finds the following: The rapidly developing array of Internet and other interactive computer services available to individual Americans represent an extraordinary advance in the availability of educational and informational resources for our citizens.").
[23] *See Schneider v. Amazon.com, Inc.*, 31 P.3d 37, 41 (Wash. App. 2001) ("Congress passed § 230 'to remove disincentives to self-regulation' created by a New York state court decision holding an ISP strictly liable for unidentifiable third parties' defamatory comments posted on its bulletin board." (quoting *Zeran v. America Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997))). *Accord Delfino v. Agilent Techs, Inc.*, 145 Cal. App. 4th 790, 807 (Cal. App. 2006) (holding that an employer is not responsible for employee's use of the workplace Internet service to make threatening comments to another person when the employer was unaware of the activity and promptly terminated the employee upon learning of the conduct).
[24] 47 U.S.C. § 230(c)(1).
[25] *Donato v. Moldow*, 865 A.2d 711, 713 (N.J. Super. Ct. App. Div. 2005).
[26] *Id.*
[27] *Id.*
[28] *Id.* at 721 (quoting 47 U.S.C. § 230(c)(2)(A)).

In light of the above concerns, the IAFF recommends that local affiliates adopt an editorial policy for any affiliate-managed webpages, including local websites and social media pages. This editorial policy would designate a process by which the local affiliate could remove any profane or inflammatory material from the local's webpages.[29] The IAFF recommends implementing a system of checks and balances in lieu of assigning this responsibility solely to one local officer. Some options include authorizing a local president to immediately remove any offensive comments, but the local president must notify the executive board of this removal. Another option would be for the local president to provide 24-hours' notice to the author of the comment before removing the comment. Another option would be a provision not allowing any member's comment to be removed without the agreement of the local president and another executive board member.

When removing any profane or inflammatory content, union leaders must be mindful of a member's rights under the LMRDA Bill of Rights, which includes the right to meet with other members and express opinions. Local affiliates **should not** remove any criticisms of the local union. There may be situations involving "mixed messages," meaning a criticism of the local union "mixed" with an inflammatory remark. In these situations, the IAFF recommends that the local affiliate reach out to the author to advise the author to repost the criticism without the inflammatory remark as the objectionable remark may open the author to potential legal liability. If the author refuses to do so after receiving such notice, the local affiliate should then remove the posting.

Can a member be held liable for the information that he/she posts on a local's web site or bulletin board?

Yes. Members must use caution when posting information to any web site or bulletin board. Defamation, a broad term which encompasses libel and slander, is the act of making a false statement to another that would harm the reputation of a third party.[30] Individuals can be held liable for defamation for posting false statements online, just as they could if they published the statements in the newspaper or made a comment in public. While opinions generally do not constitute defamation,[31] false statements about a person's profession, occupation, or official station may.[32]

Members who post to a local web site should make a reasonable effort to ensure that the information that they post is true. Although a web site may be used to discuss work conditions, members should be careful not to criticize management by making untrue or discriminatory remarks. Even though opinions do not constitute an actionable offense, a court will determine if a reasonable listener (or reader) could understand the statement as constituting a fact. Thus, if a member is not certain that the statements are true, the member should at least be clear that what

[29] For a discussion on what constitutes profane or inflammatory language, please refer to page 13 of this Manual.
[30] RESTATEMENT (SECOND) OF TORTS § 559 (1977) ("A communication is defamatory if it tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him.").
[31] *Lester v. Powers*, 596 A.2d 65, 71 (Me. 1991).
[32] *Ballard v. Wagner*, 877 A.2d 1083, 1087 (Me. 2005).

he or she is posting is only an opinion. Additionally, members will not be shielded from liability simply by not naming the person about whom they are posting. If the reader of the information would be able to discern about whom the author is speaking, the member may still be held liable if the statement constitutes defamation. Even if an online bulletin board is password protected, members should be cautious about the information they post.

Members should also be cautious not to post information that may cause another emotional distress. Lawsuits based on the intentional infliction of emotional distress can be made where the offender acted in a manner that was so outrageous that it caused another person to suffer severe emotional harm.[33] Although many courts have found that the posting of unkind material on the Internet does not rise to the level of an outrageous act for which the poster of the information can be found liable,[34] it is still best to use caution before posting information that could cause another emotional distress.[35] Local leaders may want to delete or modify any postings which they believe could potentially result in liability for one of its members.

Does my local have the right to post news and arbitration decisions on its web site or bulletin board?

Yes. A union should be allowed to post all news relating to its job on the local's web site or bulletin board, so long as the material is not confidential or otherwise lawfully shielded from public dissemination. In addition, a union may post arbitration decisions on its web site without the consent of the other party to the matter. For example, in *Providence St. Peter Hospital v. United Staff Nurse's Union Local 141*, the court denied an employer's request for an injunction to prohibit the union from posting an arbitrator's decision on its web site. The court reasoned that there have been "no prior decisions [that] support the claim that the interest of an individual company in being free from public criticism of its business practices warrants use of the injunctive power of a court," and that prohibiting the local from posting the decision would unduly restrict the union's right to freely share information with its members.[36]

It should be kept in mind that a local may want to redact certain private information from the decision before posting.

To assist affiliates in generating content for their web sites, the IAFF provides an RSS feed of related news and our blog that affiliates can subscribe to for free. (An RSS feed is a format used to publish frequently updated content such as blog entries, news headlines, audio, and video in a standardized way so that it can be distributed on more than one web site.) This can be automatically posted on affiliate web sites. If you need assistance subscribing to the RSS feeds, please contact the IAFF Information & Technology Division.

---

[33] RESTATEMENT (SECOND) OF TORTS § 46.
[34] Courts have held that mere criticism of public officials, without actual malice, is good for government and does not constitute a tortious act.
[35] *See e.g.*, *Katzenbach v. Grant*, No. 1:04CV6501OWWLJO, 2005 WL 1378976, at *18 (E.D. Cal. June 7, 2005).
[36] *Providence St. Peter Hospital v. United Staff Nurse's Union Local 141*, 2009 U.S. Dist. LEXIS 12643, 33-34 (D. Wash. 2009).

Can a local post information about an employer's policies on the local's web site or bulletin board?

It depends. Generally, a local can post information regarding an employer's employment policies on its web site. However, the First Amendment right to freely associate does not mean that members can freely and completely disregard their employer's rules in order to achieve union-related objectives. For instance, in an extreme case, *Ingham County v. Capital City Lodge No. 141 of the Fraternal Order of Police*, a court affirmed the county's decision to discipline an officer, who served as local president, for providing a copy of an internal memorandum to the union attorney without following the employer's procedures for doing so.[37] Therefore, local leaders should be careful when using the web site or bulletin board to post certain employer information or discussing union matters in a manner that would otherwise violate an employer's valid policies.

If a local maintains a web site or bulletin board, is it required to grant access to all of its members?

Generally, yes. If a local union creates a web site, it must allow all members of the union (though not usually members of the bargaining unit) the opportunity to be a part of the site, and it also must allow them to post their views therein. The LMRDA Bill of Rights expressly states that all union members shall have "equal rights and privileges within such organizations to nominate candidates, to vote in elections or referendums of the labor organization, to attend membership meetings, and to participate in the deliberations and voting upon the business of such meetings."[38] However, unions are allowed to restrict their members' speech if the restriction is "reasonably related to the protection of the organization as an institution."[39]

For example, in *Quigley v. Giblin*, a union restricted its members' access to campaign web sites by requiring members to obtain a password in order to access the sites.[40] Some members challenged this requirement, arguing that it restricted them from participating in internal elections and communicating with other members.[41] The court rejected this argument, concluding that the union could make reasonable rules to protect itself from undue outside influence.[42] Additionally, it found that passwords, which were available for all members, would not restrict their ability to remain informed, even if it would inadvertently deter some members from looking at the candidates' web sites.[43] In contrast, however, the court in *Helton v. NLRB* held that it was a violation of the National Labor Relations Act (NLRA) – which is the law

[37] *Ingham County v. Capital City Lodge No. 141 of the Fraternal Order of Police*, 739 N.W.2d 95, 102-03 (Mich. App. 2007). (holding that it was not a violation of the Public Employee Relations Act to discipline an employee who disobeyed his employer's protocol in order to advance his union's goals where there was no indication that his request for information would have been denied had he followed the proper procedures).
[38] 29 U.S.C. § 411(a)(1).
[39] *United Steelworkers of Am. v. Sadlowski*, 457 U.S. 102, 111-12 (1982) (explaining when union rules that violate interests protected in the LMRDA are valid).
[40] *Quigley v. Giblin*, 569 F.3d 449 (DC Cir. 2009).
[41] *Id.* at 454.
[42] *Id.* at 457.
[43] *Id.* at 454-55.

granting *private sector* employees the right to organize and bargain collectively, and to engage in protected concerted activity – for union officials to prohibit a member from posting criticism of the union on its bulletin board, even though it would have allowed him to post any other information on the site.[44]

While union members are permitted to criticize the union, it cannot post information that is false, defamatory, or misleading. As discussed above, defamation, a broad term which encompasses libel and slander, is the act of making a false statement to another that would harm the reputation of a third party.[45] Individuals can be held liable for defamation for posting false statements online, just as they could if they published the statements in the newspaper or made a comment in public. While opinions generally do not constitute defamation,[46] an opinion that misleads the reader into believing that a fact or statement is true might. Therefore, members who post criticism to a local's web site or bulletin board should make a reasonable effort to ensure that the information that they post is true.

In addition, local members should refrain from posting profane or inflammatory material on a local's website or bulletin board. Profanity, which includes curse words as well as racist, sexual and vulgar expressions, is generally protected by the First Amendment. However, some types of profane language are not. For instance, "fighting words," defined by the Supreme Court as words "which by their very utterance inflict injury or tend to incite an immediate breach of the peace,"[47] as well as "true threats," defined as threats to an individual's personal safety,[48] are not protected forms of speech. Similarly, speech that is inflammatory, or that advocates the use of force or law violation, is generally protected by the First Amendment, unless it is intended and likely to incite immediate lawless action.[49] Therefore, a member could be disciplined, and even subject to criminal and civil penalties, if his or her posting falls within one of these categories of speech.

Can an employer gain access to a local's web site or bulletin board without the local's permission?

Generally speaking, no. The Stored Communications Act (SCA) prohibits the unauthorized access of an interactive web site or bulletin board[50] that would allow the unauthorized person to "obtain, alter or prevent authorized access to a wire or electronic communication while it is in

[44] *Helton v. NLRB*, 656 F.2d 883, 884 (DC Cir. 1981).
[45] RESTATEMENT (SECOND) OF TORTS § 559 (1977) ("A communication is defamatory if it tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him.").
[46] *Lester v. Powers*, 596 A.2d 65, 71 (Me. 1991).
[47] *Chaplinsky v. New Hampshire*, 315 U.S. 568, 572 (1942).
[48] *Watts v. United States*, 394 U.S. 705 (1969).
[49] *Brandenburg v. Ohio*, 395 U.S. 444 (1969).
[50] *See e.g., United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2005); *Steve Jackson Games, Inc. v. United States Secret Serv.*, 36 F.3d 457, 462-63 (5th Cir. 1994); *Kauffman v. Nest Seekers, LLC*, 05 CV 6782 (GBD), 2006 U.S. Dist. LEXIS 71104, at *16-17 (S.D.N.Y. Sept. 26, 2006).

electronic storage in such system."[51] However, the statute allows a third party to gain access to the stored information if an authorized user of the site permits him or her to do so.[52] For example, in *Konop v. Hawaiian Airlines, Inc.*, the 9th Circuit indicated that an employer would not be in violation of the SCA if it accessed a password protected site, created by an employee as a forum for criticism of the union and the employer, using a password provided by an authorized user of the site.[53] Therefore, when maintaining a web site or bulletin board, local leaders should keep in mind that employers may gain access to the web site and learn information that the leaders would otherwise like to keep confidential.

Moreover, when it comes to confidential electronic communications, do not send them via e-mail. Forwarding an e-mail is easy and it happens all the time, especially with e-mails that have "confidential" notices in the subject line or in the body of the text.

To keep truly confidential information secure, post the information in a secure area of your site behind a login that is tied to a member of record and lock the information so it cannot be copied and pasted elsewhere – but do NOT send it via e-mail. You can send an e-mail out to members asking them to check the secure area of the affiliate's web site, but do not include any of the "confidential" text. If you need assistance developing security protocols for your site, please contact the IAFF Information & Technology Division.

It is important to note that local leaders may be required to disclose information posted on an interactive web site or bulletin board to a government employer if they believe that the information relates to "an emergency involving the danger of death or serious physical injury to any person."[54] Additionally, the contents of electronic communications must be disclosed pursuant to a warrant, subpoena, or court order.[55] Under these circumstances, the local operators will not be held liable for such a disclosure.[56]

Are locals required to turn over the identity of members who post anonymously on the local's web site or bulletin board to their employer?

It depends. Anonymity on the Internet exists to a certain extent. Many web sites ask users to create a "username" by which other users of the site will be able to identify them. A local can, likewise, create a web site or online bulletin board where users create and post under a username that does not need to be related to their identification. Allowing users to post comments on the Internet under pseudonyms may have the advantage of encouraging more people to freely discuss issues and conditions that concern them. Employees may feel that they can openly discuss changes they would like to see in their workplace without fearing that they will be

[51] 18 U.S.C. § 2701(a)(1). Electronic communication is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electronic, photoelectronic or photoptical system that affects interstate or foreign commerce." *Id.* § 2510(12).
[52] 18 U.S.C. § 2701(c)(2).
[53] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 880 (9th Cir. 2002).
[54] 18 U.S.C. § 2702(b)(8).
[55] *Id.* § 2703.
[56] *Id.* § 2703(e).

retaliated against for making the comments since their identity is not known.

Courts have recognized that the Internet permits anyone with access to "become a town crier with a voice that resonates farther than it could from any soapbox."[57] Therefore, in order to promote free speech, courts have extended the First Amendment's protections to anonymous speech on the Internet. However, "the anonymity of speech is not absolute and may be limited by defamation considerations."[58] If someone posts a defamatory or otherwise actionable statement on the local's web site, the person injured by the statement may be able to learn the identification of the anonymous poster. However, posters to the Internet have a right to remain anonymous and not be subject to frivolous suits filed solely for the purpose of unveiling the person's identity.[59] Consequently, most courts require the injured person to first file a law suit and post a notice of the lawsuit on the same web site where the injurious comment was posted. This gives the poster an opportunity to defend his or her statement.[60] If the person does not come forward, the court may order the web site administrator to reveal the identity of the poster if it is known and if it believes that it is likely that the statement was defamatory.[61]

Case law addressing situations in which a public employer demands that an employee/web administrator identify anonymous posters to a local's website or bulletin board is still developing. Nevertheless, it appears that an employee who administers a local's website or bulletin board and is ordered by his or her employer to turn over the identity of an anonymous poster is generally not required to do so. However, a local should immediately contact the IAFF Legal Department for assistance if such a case arises.

Finally, courts have limited the right to anonymity in the context of criminal law; however, that complex discussion is beyond the scope of this manual.

[57] *Reno v. ACLU*, 521 U.S. 844, 870 (1997).
[58] *Indep. Newspapers, Inc. v. Broadie*, 407 Md. 415, 430 (Md. Ct. App. 2009) (citing *Beauharnais v. Illinois*, 343 U.S. 250, 266 (1952)).
[59] *Id.* at 443.
[60] *See, e.g.*, *Doe v. Cahill*, 884 A.2d 451, 460 (Del. 2005).
[61] *See Moblisa, Inc. v. Doe*, 170 P.3d 712 (Ariz. Ct. App. 2007); *Sony Music Entm't, Inc. v. Does 1-40*, 326 F. Supp. 2d 556 (S.D.N.Y. 2004).

Employer Internet Policies

I. Frequently Asked Questions

Can an employer's Internet or e-mail policy be used as evidence of anti-union discrimination?

Yes. An employer may not harass or discriminate against union members through regulation or enforcement of an Internet or e-mail policy. Employers must treat union and non-union members equally.[62] If employees can prove that the employer enforces the Internet policy and disciplines union members more strictly than it does non-union members, this conduct can be used as proof of a violation of the First Amendment, as well as federal and state laws prohibiting employers from harassing or retaliating against members for their union activity. The degree of protection depends on whether an employee is protected by a bargaining statute, a contract, or only the Constitution.

For instance, in 2014, the National Labor Relations Board (NLRB), which governs *private sector* labor disputes, addressed employee use of employer e-mail systems to engage in protected concerted activities. The Board issued a decision in this case, *Purple Communications*, and created a presumption that "employees who have rightful access to their employer's email system in the course of their work have a right to use the email system to engage in [protected concerted communications] on nonworking time."[63] In addition, in 2005, the NLRB issued a decision in *Southern California Gas Company and Utility Workers Union of America Local 132 AFL-CIO*, finding that it was a violation of the National Labor Relations Act (NLRA) for an employer to discipline an employee for using the employer's e-mail system to send union announcements.[64] In this case, Southern California Gas Company allowed its employees to use the company e-mail system for appropriate non-business or personal use so long as it did not interfere with the employee's ability to perform his or her job or the company's mission, and so long as it was not used for objectionable activities, such as to threaten or harass another employee. The NLRB explained that the employer unlawfully discriminated against the employer based on his union activity because other company employees were not disciplined for sending similar e-mails concerning non-business social gatherings.[65]

In 2010, the NLRB filed an unfair labor practice complaint against American Medical Response of Connecticut, Inc. (AMR) alleging the company illegally terminated an employee who posted

[62] For example, the U.S. Court of Appeals for the Fourth Circuit affirmed a National Labor Relations Board (NLRB) decision where an employer had a policy of banning photography at the workplace. An employee took pictures with her cellphone camera to document the employer's inconsistent enforcement of a dress code banning hats, where women were more frequently disciplined under this policy than men. The Fourth Circuit held that the employee's taking of cell phone pictures and showing them to others constituted protected concerted activity. Furthermore, the fact that the employer irregularly enforced the photography ban weighed in the employee's favor. *NLRB v. White Oak Manor*, 452 F. App'x 374, 376 (4th Cir. 2011).
[63] *Purple Communications*, 361 NLRB No. 126, slip op. at 14 (Dec. 11, 2014).
[64] *Southern California Gas Company and Utility Workers Union of America Local 132 AFL-CIO*, 21-CA-36039, 2005 WL 2438516 (Sept. 14, 2005).
[65] *Id.*

negative comments about her supervisor on the employee's personal Facebook page. Coworkers also posted messages in response supporting the employee, and the employee in turn posted more negative comments about the supervisor. AMR suspended and then terminated the employee alleging that the postings violated AMR's internet policies, which prohibit employees "from making disparaging, discriminatory or defamatory comments when discussing the Company or the employee's superiors, co-workers and/or competitors." The employee's union filed an unfair labor practice charge over the discipline. The NLRB investigated and found that the employee's Facebook posts constituted protected activity under the National Labor Relations Act (NLRA), and that AMR's internet policy contained illegal provisions that interfered with AMR's employees exercising their right to engage in protected, concerted activity under the NLRA. The case settled before it went to a hearing, but as part of the settlement AMR agreed to amend its policy.

The NLRB continues to be at the forefront of protecting employees' speech rights on social networking sites. Recently, the Board held that an employer violated the Act when it terminated two employees for engaging in a discussion on Facebook and using profanity to criticize the employer for its failure to withhold the correct amount of state income tax from their paychecks.[66] The Board found that these communications were protected concerted activity because the employees were looking towards group action to address their terms and conditions of employment.[67]

If a member believes that he or she is being retaliated or discriminated against based on his or her union activity, he or she should immediately contact a local officer for assistance.

Can a local use the employer's web site as evidence of anti-union retaliation?

Depending on the content of the site, a local may be able to use the employer's web site as evidence of retaliation. Courts are frequently allowing material posted online to be offered into evidence in both civil and criminal trials. Additionally, the local may be able to use a management official's personal Facebook or social networking page as evidence that he or she harbored animosity against members of the union. For example, any jokes or mean-spirited remarks that managers post to these web sites can be used as evidence of anti-union animus. Similarly, if a manager or employer maintains a blog or company newsfeed and only reports on incidents involving union members, this conduct may be used as evidence that the employer tends to discipline union members more often than non-union members.

Just as employers may monitor an employee's personal web site or social networking page, local members who suspect that they have been unfairly retaliated against should monitor their employers' and managers' online activity.

[66] *Triple Play Sports Bar and Grille*, Nos. 34-CA-012915, 34-CA-012926 (N.L.R.B. Aug. 22, 2014).
[67] *Id.*

Who owns the footage derived from the use of personal helmet cameras – the fire fighter or the Fire Department? Can the Fire Department demand that the fire fighter turn over this footage?

Members are increasingly using personal helmet cameras while on duty, which raises a number of legal questions regarding the footage produced by the camera. One frequent question concerns whether the fire fighter or the Fire Department owns this footage. It appears that many courts and state legislatures have not yet addressed this issue, so the law on these issues is currently unclear. Furthermore, the Fire Department may want to access these videos for its own purposes, including for training or for defending itself against a lawsuit. Another question, therefore, involves whether the Fire Department can demand access to this footage under the Fourth Amendment of the U.S. Constitution or pursuant to any public records laws in the state. This is another largely unanswered question.

There does not appear to be any on-point case law involving helmet cameras, but there are informative cases on the use of personal cell phones. For example, the Court of Appeals of New Mexico affirmed a lower court ruling granting a motion to compel a police officer's personal cell phone records during a traffic stop because these records "were in control of the State because they were in the possession of the officer during the time in question." The Court affirmed the lower court's decision finding that the police officer was an arm of the state, and therefore his private phone records were in the possession, custody, or control of the state, making them subject to public disclosure rules. *State v. Ortiz*, 146 N.M. 873, 879 (N.M. Ct. App. 2009). In a Washington state case, the Court of Appeals held that a prosecutor's personal cell phone records and text messages were considered public records under the Washington Public Records Act only regarding those calls related to government business and only if the records were used or retained by the government. *Nissen v. Pierce County*, 183 Wn. App. 581, 596 (Wash. Ct. App. 2014).

In light of this legal ambiguity, the IAFF recommends that locals negotiate the use of personal helmet cameras with the employer and incorporate this language into the collective bargaining agreement or memorandum of understanding. If locals resolve these issues upfront, local members and the Fire Department can set out clear expectations regarding the use of helmet cameras. The contract provision should include a clause granting authorization to use personal helmet cameras; for example, the contract could state that a member's use of a personal helmet camera while on duty shall be subject to the approval of the shift supervisor. The IAFF recommends that the local grant the employer a limited license to this footage. The contract language should state that a copy of any footage or other recorded media derived from the use of a personal helmet camera shall be produced to the Fire Department upon request only for official purposes. The language should further clarify that any footage provided by the local or its members to the Fire Department shall not be released to the public unless pursuant to a court order or some other legal obligation, such as public records laws. This language should also make clear that in any case, the employee shall retain ownership of the footage, with absolutely no exceptions.

Members, however, should exercise caution when using helmet cameras and when posting any footage derived from the camera to the Internet. Members should seek legal advice to ensure that posting or deleting this footage does not violate any laws, such as the Health Insurance Portability and Accountability Act (HIPAA), evidentiary laws, and privacy laws, which vary state by state.

Participation in Social Networking Sites

I. Frequently Asked Questions

What are the risks involved in maintaining personal web sites and joining social networking sites such as Facebook, MySpace, or Twitter?

Although social networking and blogging web sites have become more popular and mainstream, and indeed the IAFF and many affiliates already have developed such sites, there are significant risks associated with belonging to these sites. Unless special protections are put in place, information that is posted on the Internet is available for anyone to see. Even information that is "deleted" from a web site may still be accessible. Therefore, members should be cautious when they post information to any of these sites. Although the employer generally should not expect to be able to control employees' use of these sites during their free time, employees should still be aware that there may be repercussions for the information that they post while off-duty. Moreover, courts have been unwilling to find that employees have a reasonable expectation of privacy with regard to information that an employee voluntarily posts online.[68]

In a First Amendment case, the Supreme Court has recognized that, "when someone who is paid a salary so that she will contribute to an agency's effective operation begins to do or say things that detract from the agency's effective operation, the government employer must have some power to restrain her."[69] As discussed above in greater detail, to determine if a public employee can be disciplined for his or her speech, the court will first ask if the speech related to a matter of public concern. If the speech solely relates to a personal grievance, it may not be protected by the First Amendment. Courts have ruled that at least some speech on social networking sites is protected by the First Amendment. For example, in *Bland v. Roberts*, a deputy sheriff "liked" his boss's opponent's election Facebook page, and he was not reappointed after his boss won reelection. The 4th Circuit held that the deputy sheriff's liking of the candidate on Facebook was expressive activity and is thus considered protected speech under the First Amendment.[70]

If the speech is a matter of public concern, the court must next ask if the speech could potentially disrupt the employer's operations. If the court finds that the disruption to operations outweighs the employee's right to speak freely, the employee's speech is not protected.[71]

---

[68] *See* Sharon Nelson, et. al., *The Legal Implications of Social Networking*, 22 REGENT U.L. REV. 1, 21 (2010). .
[69] *Waters v. Churchill*, 511 U.S. 661, 674 (1994).
[70] *Bland v. Roberts*, 730 F.3d 368, 381 (4th Cir. 2013).
[71] In Canada, when addressing employee discipline for social media-related conduct, arbitrators assess whether the conduct harms the employer's reputation. Arbitrators then evaluate whether the social media postings have a real and material connection to the workplace, and whether the employer's concerns about the impact of the postings on its reputational interest were substantial and warranted. Regarding privacy concerns, arbitrators have noted that privacy and secrecy can never be guaranteed for social media websites. *City of Toronto v. Toronto Professional Firefighters Association, Local 3888*, (2014) F13-142-07, 2014 CanLII 62879, p. 32-33 (ON LA) (Misra) (arbitrator rescinded a fire fighter's termination based on comments about women made on Twitter and instead substituted a three-day suspension). Arbitrators also examine the nature and frequency of social media postings and whether the comments were so damaging or have so poisoned the workplace that it would no longer be possible for the

At least thirty states have legislation that protects employees' off-duty conduct. Some statutes protect an employee's ability to smoke tobacco products off-duty, while other more liberal statutes provide employees with greater rights regarding their off-duty conduct. Nevertheless, even the most progressive laws regarding off-duty conduct contain exceptions for conduct that is contrary to the business interests of the employer.[72] Therefore, an employee's off-duty tweets and status updates criticizing an employer or complaining about his or her job could result in discipline if they interfere with an employer's business interests.

Further, some states have enacted laws specifically allowing public employees to be disciplined for off-duty conduct that conflicts with their state duties or is unbecoming of an employee.[73] For example, in *In re Nicosa*, the court upheld the termination of a New Jersey state employee who was upset with his town's police department and later fired for posting comments in an online chatroom that encouraged others to shoot policemen.[74]

Under the NLRA, the private sector statute, union members, or employees in general, may be afforded some protection for their online comments if they can prove that the comments are protected concerted activity. For concerted activity to be protected, the employees must have been engaged in a conversation with the intent to initiate, induce, or prepare for group action.[75] Employees participating in a local's online bulletin board or chatroom will likely be protected under the NLRA. Additionally, the NLRB has extended concerted activity protection to employee e-mails that proposed changes to the employer's policies.[76] The NLRB has also extended concerted activity protection to social media websites,[77] in particular to an employee Facebook post criticizing the manner in which his employer, a car dealership, conducted and catered a sales event.[78] The NLRB found that these postings were protected concerted activity because the postings were about the impact of the manager's poor food choices on the employees' ability to sell cars. In this case, however, the NLRB found that the employer terminated the employee for another unflattering Facebook post unrelated to the sales event. In this post, the employee posted a photo of an incident at another dealership owned by the manager where the dealership allowed a 13-year-old to sit in the driver's seat of a car. The 13-year-old proceeded to drive the car into a pond. The NLRB found that this posting was not protected concerted activity because it had no connection to the employees' terms and conditions of

---

employee to work harmoniously and productively with other employees or for the employer. *Bell Technical Solutions v. CEP (Facebook Postings Grievance)* (2012), 224 L.A.C. (4th) 287.

[72] *See, e.g.*, N.Y. Lab. Law 201-d(3)(a).

[73] *See, e.g.*, N.J. Admin. Code § 4A:2-2.3(a)(6).

[74] *In re Nicosa*, 2007 N.J. Super. Unpub. LEXIS 1123 (N.J. May 17, 2003).

[75] *Mushroom Transp. Co. v. NLRB*, 330 F.2d 683, 685 (3d Cir. 1964); *Hispanics United of Buffalo*, NLRB Case No 03-CA-027872 (2012) (finding Facebook postings by five employees chastising a fellow employee who initially criticized the work of the five employees by text message to be protected concerted activity because they were taking group action to defend themselves against the accusations made by the other employee).

[76] *Timekeeping Systems*, 323 NLRB 244 (1997).

[77] *Murphy Oil USA, Inc.*, 361 NLRB No. 72 at *19 (2014) ("the use of modern communication technologies such as social media to pursue unionization is obviously protected, regardless of whether workers during the Depression has access to Facebook").

[78] NLRB Case No. 13-CA-46452 (2011).

employment.[79] One thing to keep in mind, however, is that blogs or postings which would otherwise be considered concerted activity may lose their protection if the content is abusive, insubordinate, or disloyal.[80] In addition, social media postings that amount to individual complaints do not receive this protection.[81]

Obviously, union members generally enjoy greater protections with regard to online speech if a collective bargaining agreement is in place requiring that an employer have "just cause" prior to disciplining an employee. For instance, in *Land v. L'Anse Creuse Public School Board of Education*, a middle school teacher was fired after the school board discovered a picture of her at a bachelorette party that was posted to the Internet without her knowledge. The school board determined that the picture represented moral turpitude that was unbecoming of an educator; however, the State Tenure Commission, whose decision was upheld by the Michigan Court of Appeals, found that just cause for termination could not be based solely on a teacher's off-duty conduct that did not involve the students and did not affect her ability to teach.[82]

Finally, it is important to note that these greater protections may only exist in limited circumstances. Therefore, members must still be extremely careful when posting any information online.

Can a public employer require its employees to provide their personal e-mail, Facebook, MySpace, or Twitter passwords, or access these accounts without the permission of the employee?

The answer appears to be no.[83] Nevertheless, while some courts have found that employers are able to monitor and search personal e-mail accounts sent using an employer provided

---

[79] *Id.*

[80] *See NLRB v. Int'l Brotherhood of Elec. Workers*, 346 U.S. 464 (1953) (holding that an employee could be discharged for being critical of the company's product while trying to engage other union members to attempt to reform the company's working conditions); Rafael Gely & Leonard Bierman, *Social Isolation and American Workers: Employee Blogging and Legal Reform*, 20 HARV. J. LAW & TEC 288, 310-11 (2007). *But see Three D, LLC*, 361 NLRB No. 31, slip op. at 3-4 (2014) (the Board found that employees' Facebook activity was protected concerted activity – where one former employee complained about owing additional taxes and about the employer's bookkeeper who was also a co-owner and later posted that she could call "the labor board to look into it," another current employee "liked" the post, and another current employee noted that she also owed taxes and called the co-owner "an asshole" – and the Board rejected the employer's argument that this discussion impermissibly disrupted the work environment and therefore lost any such protection).

[81] *See, e.g.*, *Helser Indus.*, NLRB Div. of Advice, No. 19-CA-33145 at 33 (2011) (employee's posts on Facebook stating that he was angry that a coworker reported him for causing an accident with work equipment were not protected concerted activity and were instead "an expression of an individual gripe").

[82] *Land v. L'Anse Creuse Public School Board of Education*, 2010 Mich. App. LEXIS 999 (Mich. Ct. App. 2010).

[83] States have been introducing legislation since 2012 to prevent employers from demanding passwords to their employees' social media accounts. As of the publication of this manual, legislation has been introduced or is pending in at least 28 states, and legislation banning this practice to varying extents has been enacted in Louisiana, Maine, New Hampshire, Oklahoma, Rhode Island, Tennessee, Wisconsin, Arkansas, Colorado, Illinois, Nevada, New Jersey, New Mexico, Oregon, Utah, Vermont, Washington, California, Delaware, Maryland, and Michigan. National Conference of State Legislators, *Employer Access to Social Media Usernames and Passwords*, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx (last accessed on October 9, 2014).

computer,[84] employees generally have a reasonable expectation of privacy while sending e-mails through their private, password protected e-mail account. For instance, in *Stenghart v. Loving Care Agency*, the court held that, although an employer may enforce lawful policies regarding e-mail use by employees while at work, this does not mean that the employer has access to the privileged contents of any e-mail sent by the employee through their private e-mail account during work hours or on an employer's computer.[85] This protection would likely extend to an employer's demand for the password to an employee's personal Facebook, MySpace, or Twitter accounts, as well as to messages sent privately using these services.

Additionally, a private employer who has illegally accessed an employee's personal online accounts may be held liable for invasion of the employee's privacy. This cause of action is only available, however, if the employee was somehow harmed, and took precautions to limit the number of people who could view the account. For instance, if an employer gains access to a "tweet" or a blog posting, it is unlikely that the employee would be able to recover because the information could potentially be accessed by any member of the public.

Finally, under these circumstances, both private and public employees may be able to bring suit under the Stored Communications Act (SCA), which prohibits the unauthorized use or access of another person's electronic communications. However, because the SCA allows the provider of the Internet service to access this information, an employee would not be able to sue under this law if he or she were using the employer's e-mail or Internet services.[86] Nevertheless, local members could succeed in suit under the SCA if the employer accessed an e-mail that was not sent using the employer's e-mail, or illegally gained access to a members-only section of a local's web site. For example, in *Konop v. Hawaiian Airlines, Inc.*, the 9th Circuit indicated that an employer violated the SCA when it accessed an employee's online bulletin board using login information provided by employees who, although authorized, were not in fact users of the site. The court explained that by intentionally accessing the stored electronic communication without proper authorization, the employer acted illegally.[87]

It is also important to note that most social networking sites have privacy controls that enable a user to significantly restrict who has access to the information posted on their personal page on that site. If a member fails to take advantage of these privacy tools, the default setting set by the social networking site is generally to make everything public. So, it is important to advise members to carefully select their privacy settings on social networking sites.

---

[84] *See Stenghart v. Loving Care Agency, Inc.*, 990 A.2d 650, ***9-10 (N.J. 2010).
[85] *Id.*; *see also Thygeson v. U.S. Bancorp*, No. CV-03-467-ST, 2004 WL 2066746, at *22 (D. Or. Sept. 15, 2004) (holding that there is a heightened expectation of privacy in personal e-mail accounts, but those accounts may be monitored where an explicit policy exists; however this does not necessarily allow the employer to search the content of the e-mails sent and received).
[86] 18 U.S.C. § 2701. *See also* Clifford S. Fishman, *Technology and the Internet: The Impending Destruction of Privacy by Betrayers, Grudgers, Snoops, Spammers, Corporations and the Media*, 72 GEO. WASH. L. REV. 1503, 1529 (2004).
[87] *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002).

Privacy Rights

I. Frequently Asked Questions

Does an employer have the right to access information contained on a cell phone, laptop, or smartphone/iPhone provided by the employer?

Generally speaking, yes, in contrast to cell phones, iPhones, or other electronic communication devices owned and used solely by the employee. It is not unlawful for an employer to monitor employees' e-mail or Internet usage while the employee is using a work computer, e-mail, or Internet service. The Federal Wiretap Act prohibits the interception and disclosure of wire, oral, or electronic communications of another person.[88] The statute contains an exception where there is consent.[89] Courts have broadly construed this exception, only requiring that consent be implied or "inferred 'from surrounding circumstances indicating that the party knowingly agreed to the surveillance.'"[90] Thus, if an employee has reason to know about an employer's monitoring policy, the employer may monitor the employee's e-mail and discipline the employee for inappropriate use without violating the Act.

The Fourth Amendment protects individuals from unreasonable searches and seizures, but it only applies when the government acts. If a private citizen or employer invades the privacy of another, no Fourth Amendment claim can be made; however, there may be other common law or statutory remedies available when private employers act in such a manner.[91] In order to be protected by the Fourth Amendment, the person must have had a reasonable expectation of privacy with regard to the item/place that is searched or seized.[92] In *O'Connor v. Ortega*, the Supreme Court recognized that "the operational realities of the workplace…may make *some* employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement officer."[93] The operational realities may include the employer's practices and policies, or the fact that business records are subject to public disclosure laws. The court went on to note that "in the case of searches conducted by a public employer, we must balance the invasion of the employees' legitimate expectations of privacy against the government's need for supervision, control, and efficient operations of the workplace."[94]

---

[88] 18 U.S.C. § 2511.
[89] *Id.* § 2511(2)(c).
[90] *Sporer v. UAL Corp.*, No. C-08-02835 JSW, 2009 WL 2761329, at 6 (N.D. Cal. Aug. 27, 2009) (quoting *Griggs-Ryan v. Smith*, 904 F.2d 112, 117 (1st Cir. 1990)). Keep in mind, however, that under the NLRA, the employer may not engage in surveillance targeted towards employees' union activities. *See Purple Communications, Inc.*, 361 NLRB No. 126, slip op. at 15-16 (2014) ("[a]n employer's monitoring of electronic communications on its email system will similarly be lawful so long as the employer does nothing out of the ordinary, such as increasing its monitoring during an organizational campaign or focusing its monitoring efforts on protected conduct or union activities").
[91] A common law claim against a private employer can be made. There are generally four common law claims that can be made: 1) intrusion upon seclusion, 2) public disclosure of embarrassing private facts, 3) false light in the public eye, and 4) commercial appropriation of a name or likeness.
[92] *O'Connor v. Ortega*, 480 U.S. 709, 715 (1987) (Without a reasonable expectation of privacy, a workplace search will not violate the Fourth Amendment, regardless of the search's nature and scope.).
[93] *Id.* at 737.
[94] *Id.* at 719-20.

While some courts have found that an employee has a reasonable expectation of privacy when transmitting information using his or her employer's e-mail system or computer,[95] the majority of decisions affirm an employer's right to search these electronic communications. In *In re Asia Global Crossing, Ltd.*, the court developed four factors for courts to consider when determining if an employee has a reasonable expectation of privacy: (1) whether the company maintains a policy banning personal or other objectionable use; (2) whether the company monitors the employee's use of e-mail or the computer; (3) whether third parties have a right to access either the computer or the e-mails; and (4) whether the employee was notified by the company or otherwise aware of the company's monitoring policies.[96]

In *City of Ontario v. Quon*, the Supreme Court upheld a public employer's search of the text messages sent by a police officer using an employer provided alphanumeric pager. The Court explained that the officer did not have a reasonable expectation of privacy in the text messages, even where the department had not been enforcing its formal policy that text messages and other electronic communications could be monitored, and the officer had been paying for text messages that fell outside of the employer's text messaging plan. The Court noted that, "as a law enforcement officer, he would or should have known that his actions were likely to come under legal scrutiny, and that this might entail an analysis of his on-the-job communications."[97]

In contrast, while some courts have found that employers are able to monitor and search personal e-mail accounts sent using an employer provided computer,[98] employees generally have a reasonable expectation of privacy while sending e-mails through their private, password protected e-mail account. For instance, in *Stenghart v. Loving Care Agency*, the court held that, although an employer may enforce lawful policies regarding e-mail use by employees while at work, this does not necessarily mean that the employer may access the contents of any e-mail sent by the employee during work hours or on an employer's computer.[99]

Even if the employee has a reasonable expectation of privacy, courts have allowed government employers to search the workplace and the employee's e-mail when the search involves work-related misconduct.[100] However, the search must be justified at its inception, meaning that there are reasonable grounds to believe that the search will produce evidence of the misconduct, and it must be limited in its scope and not excessively intrusive.[101]

---

[95] *See e.g., Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 101 (E.D. Pa. 1996); *see also Brown-Criscuolo v. Wolfe*, 601 F. Supp. 2d 441, 449 (D. Conn. 2009) (holding that even though the public employee was aware of a routine monitoring policy, there was a reasonable expectation of privacy because the e-mail accounts were password protected and the employer did not often monitor them).
[96] *In re Asia Global Crossing Ltd.*, 322 B.R. 247, 257-58 (Bankr. S.D.N.Y. 2005).
[97] *City of Ontario v. Quon*, 560 U.S. 746, 762 (2010).
[98] *Stenghart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010).
[99] *Id.*; *see also Thygeson v. U.S. Bancorp*, No. CV-03-467-ST, 2004 WL 2066746, at *22 (D. Or. Sept. 15, 2004) (holding that there is a heightened expectation of privacy in personal e-mail accounts, but those accounts may be monitored where an explicit policy exists; however this does not allow the employer to search the content of the e-mails sent and received).
[100] *Leventhal v. Knapek*, 266 F.3d 64, 75-76 (2d Cir. 2001).
[101] *Id.* at 75 (citing *O'Connor*, 480 U.S. at 726).

Arbitrators have also found that companies and government employers are permitted to monitor their employees' use of its Internet or e-mail. Generally, a violation of a company's e-mail policy can lead to progressive discipline.[102] In some cases, where the violation is egregious, arbitrators have permitted the employer to skip progressive discipline and terminate the employee outright.[103] However, where a collective bargaining agreement is in place, the employer must abide by the terms of that agreement when disciplining an employee for violating an employer's Internet or e-mail policy.

Finally, fire fighters who are required to respond to emergencies should expect that their on-the-job communications may be analyzed. This may be the case even if the employees are not using a device provided by the employer, as discussed in greater detail below. Additionally, the actions and activities of public safety employees immediately preceding or during an emergency may come under greater scrutiny, thus lowering the reasonable expectation of privacy for these employees.

Does a public employer have the right to access information contained on an employee's personal cell phone, laptop, or smartphones/iPhone?

When an employee uses his own personal items, such as a cell phone or laptop, at work, he has a more heightened expectation of privacy. The Supreme Court has stated that ownership over an item is a factor to consider when determining whether one's Fourth Amendment rights have been violated.[104] However, if the employee uses his or her own device, but gains access through the employer's Internet, the employer will be able to access the information that is in storage in the same way that it can when the employee uses the employer's computer.

Generally speaking, government employers are not permitted to access the *information* contained on an employee's personal device. For instance, in *Stenghart v. Loving Care Agency*, the court stated that employers may enforce e-mail policies, but they "have no need or basis to read specific *contents* of personal, privileged, attorney-client communications in order to enforce corporate policy."

However, as noted above, even if the employee has a reasonable expectation of privacy, courts have allowed government employers to search the workplace and the employee's e-mail when

[102] *But see In re City of Quincy & Firefighters, Local 63, 1.A.F.F*, 126 Lab. Arb. Rep. 767 (2008) (Finkin, Arb.) (holding that a continued knowing violation of the city's e-mail policy by sending personal e-mails to a lover did not constitute just cause to discharge the employee); *In re Ga. Power Co.*, 123 Lab. Arb. Rep. 936 (2006) (Nolan, Arb.) (finding that there was no just cause to discharge an employee where the only violation of company policies during a long career with the company was the Internet usage violation).
[103] *A.E. Staley*, 119 Lab. Arb. Rep. 1371 (2004) (Nathan, Arb.) (finding that distributing pornography through the company's e-mail was a gross violation of the company's policy and would reflect poorly on the company, so dismissal was appropriate).
[104] *United States v. Salvucci*, 448 U.S. 83, 91 (1980) (holding that an illegal search only violates the rights of those with a legitimate expectation of privacy in the place searched).

the search involves work-related misconduct.[105] When analyzing searches of employee's personal communications, courts have often stated that the employer is allowed to know to whom the information was sent as well as the general topic of the information, but they are not always allowed to read or listen to the content of the communication. However, if the employee is using his personal device in a way that is detrimental to the employer, the court may allow a search which is reasonably expected to produce evidence of wrongdoing if it is limited in its scope.[106] The U.S. Supreme Court case, *City of Ontario v. Quon*, indicates that the court is more willing to allow the employer to have access to the information if it is necessary in investigating the wrongdoing.

Additionally, an employer may be able to access the information contained on a personal device where the employee allows other employees access to the device. For instance, in *United States v. Barrows*, a government employee brought suit when his employer reviewed the documents contained on his personal laptop. The employee connected his personal computer to the government's network, routinely left his computer on in his office without a password, and was aware that other employees knew his password and occasionally used his laptop. The court held that although the employee had a subjective expectation of privacy when he used his personal computer at work, the employer did not violate his 4th Amendment privacy rights because he failed to take precautions to prevent other co-workers from viewing his files.[107] To be careful, affiliate leaders should urge their members to be cautious not to leave their electronic devices in public areas where others may be able to access them.

If the employee does not use a personal device while at work, but merely has it with him or her, it is unlikely that the employer will be able to access the information contained on the device. Courts have stated that merely having a personal item in the workplace does not make it part of the workplace, and therefore, the employee does not lose his or her expectation of privacy simply by bringing it with him or her to work.

[105] *Leventhal v. Knapek*, 266 F.3d 64, 75 (2d Cir. 2001) (finding that, even though employee had some expectation of privacy in the contents of his workplace computer, the searches were reasonable in light of the employer's need to investigate allegations of misconduct as balanced against the intrusion caused by the search).
[106] *See O'Connor*, 480 U.S. at 726.
[107] *United States v. Barrows*, 481 F.3d 1246, 1249 (10th Cir. 2007).

Ownership Rights and Local Web Sites

I. Frequently Asked Questions

What action can locals take if another party registers a web address that is similar to the local's web address?

If a local union wishes to create a web site, it will need to register for an Internet Protocol (IP) address and a domain name. The Internet Corporation for Assigned Names and Numbers (ICANN) is the non-profit corporation tasked with maintaining the database of registered domain names. As more and more organizations, corporations, and individuals seek to expand their presence online, there is competition for domain names. In order to profit, or even harass, companies and organizations, "cybersquatters," buy or register domain names utilizing trademarks or other well-known names associated with others. If it is not possible to buy the exact name, cybersquatters often buy a similar name to confuse consumers or information seekers. This is a new and developing field, so aside from trying to negotiate or buy the domain name, there are two main avenues available to remedy "stolen" web site addresses or Uniform Resource Locators (URLs).

- **Uniform Domain Name Resolution Policy**

ICANN has created a procedure, similar to arbitration, which seeks to resolve domain name disputes. This process is preferred by many parties due to its brevity. Through this process, a complainant submits a complaint to any ICANN approved Provider. The complaint should describe how the domain name is identical or similar to a trademark or service mark to which the complainant has a right, why the current domain holder should be considered to have no right, and why the domain name should be considered to have been registered in bad faith.[108] The complainant must also indicate what relief is sought, what other legal proceedings have been commenced regarding the action, and whether he or she is requesting a one or three person panel.[109] The complainant must also send a copy of the complaint to the party alleged to have "stolen" the domain name in accordance with ICANN's policy statement.[110] If the Provider finds the complaint to be deficient, he or she shall notify the complainant that he or she has five days to correct the deficiencies. If an administrative proceeding commences, the Respondent has twenty days from that date to submit a response to the Provider. The Respondent has the opportunity to request that the case be heard by a three-person panel. Both parties are allowed to submit up to three names of potential panelists. The Provider will then select independent

[108] ICANN, Uniform Domain Name Resolution Policy, ¶ 3(ix)(1)-(3), https://www.icann.org/resources/pages/rules-be-2012-02-25-en(last accessed October 8, 2014). There are additional word and page limits that the Providers may place on the complaint. Any complainant should check the Provider's Supplemental Rules to ensure that the complaint is compliant.

[109] *Id.*

[110] *Id.* ¶ 2. The complainant should make every effort to send a copy of the complaint to the alleged violator. The complainant should send the complaint to every postal-mail and facsimile addresses shown in the Registrar's database for the registered domain-holder and the administrative and technical contacts. *Id.* ¶ 2(a)(i). The complainant should also send the complaint by e-mail to those addresses listed with the Registrar, to any e-mail addresses on an active web site and to postmaster at the domain name (postmaster@<domainname>). *Id.* ¶ 2(a)(ii).

panelists. The panel has great flexibility in deciding the case. It is not required to hold in-person hearings, except in exceptional cases. The panel is to make a decision within fourteen days of its appointment. If the panel decides the domain name should be cancelled, it will inform ICANN.[111] ICANN will wait ten business days before taking any action to allow the losing party to commence a lawsuit. If a lawsuit is not filed within ten days, ICANN will cancel the domain name.

- **Filing a Domestic Lawsuit**

The Anticybersquatting Consumer Protection Act creates liability for a person who – in bad faith with intent to profit – registers, traffics, or uses a domain name that is identical or confusingly similar to a distinctive or famous mark that is registered to another person or company.[112] The Act specifies that a personal name is included in the scope of this protection.[113] If the user of the domain name is not subject to the court's personal jurisdiction or cannot be located, the Act allows the owner of the mark to file a law suit that seeks cancellation of the domain name as it is being used by the cybersquatter.[114] Locals may have difficulty pursuing this option because it is only available to the holders of a famous or distinctive trademark. Additionally, the site that is stolen must be used for profit. If neither of these conditions is met, no lawsuit can be filed under this provision.

[111] ICANN, Uniform Domain Name Dispute Resolution Policy, ¶ 4(k), https://www.icann.org/resources/pages/policy-2012-02-25-en (last accessed October 8, 2014).
[112] 15 U.S.C. § 1125(d).
[113] *Id.* § 1125(d)(1)(A). Further protection for individual names is provided in 15 U.S.C. § 8131.
[114] *Id.* § 1125(d)(2)(A).

Public Records Statutes

I. Frequently Asked Questions

Are Internet records, such as e-mails, subject to disclosure under public records statutes?

Because it is important that citizens have access to government records in order to hold their elected and non-elected officials accountable, many states (as well as the federal government) have enacted public records statutes. These statutes make the information produced by the state (or a political subdivision thereof) available to the public if the information relates to a matter of public concern or the carrying out of government business. Therefore, an employee's e-mails, text messages, and Internet records may be subject to disclosure under these laws if they involve the execution of a state or municipality's duties. Courts have been liberal in determining what material is subject to the public record statutes; however, not all Internet or e-mail records must be made available. As the court in *Denver Publishing Co. v. Board of Commissioners of Arapahoe County* stated, "the fact that a public employee or public official sent or received a message while compensated by public funds or using publicly-owned computer equipment is insufficient to make the message a 'public record.'"[115]

Nevertheless, fire fighters and locals should be cautious when sending work related e-mails or posting information on the Internet. Even casual e-mails sent between employees or to a supervisor can be subject to disclosure.[116] In addition, any Internet searches that relate to the functioning or operation of the fire department may become part of the public record. Moreover, if an individual is denied membership in the union or alleges an unfair labor practice by a local, he or she may be able to gain access to e-mails or Internet records of union members through public disclosure statutes.

Even electronic communications that do not relate specifically to fire department business may also fall under public record statutes. In *Tiberino v. Spokane County Prosecutor*, the court found that personal e-mails sent from a work computer were part of the public record when the employee was fired based on her inappropriate use of the Internet.[117] The court held that the e-mails were subject to the public record statute because the firing and hiring of employees was a legitimate function of the government and the public had a right to information relating to this process.

Furthermore, courts may determine that a firefighter's use of electronic communications immediately before or during the time when he or she is responding to an emergency is considered part of the public record, and therefore subject to disclosure. Firefighters should be

[115] *Denver Publ'g Co. v. Bd. of Comm'rs of Arapahoe County*, 121 P.3d 190, 199 (Colo. 2005) (holding that personal e-mails exchanged between employees were not subject to the public disclosure statute).
[116] *Cowles Publ'g Co. v. Kootenai County Bd. of County Comm'rs*, 159 P.3d 896, 900-01 (Idaho 2007) (holding that a series of e-mails sent between an employee and a supervisor were part of the public record even where some of the e-mails were of a personal nature).
[117] *Tiberino v. Spokane County Prosecutor*, 13 P.3d 1104, 1108 (Wash. App. 2000).

dissuaded from using a cell phone or electronic device for personal reasons while responding to an emergency, unless necessary or appropriate under the circumstances.

Affiliates should also be careful when collecting member e-mail addresses to not include e-mail addresses owned by the employer. When asking members for their e-mail address, request their personal e-mail, not the one they obtained from their employer.

Finally, most states include exemptions to the public record laws where the information would be highly embarrassing or offensive to the individual were it disclosed.[118] Therefore, if there is no legitimate or reasonable public interest in the information, it should be redacted from the record.

For more detailed information on public records laws, please refer to the IAFF Freedom of Information Act Manual.

[118] *See, e.g.*, WASH. REV. CODE § 42.17.255.

Collective Bargaining and Internet/E-mail Policies

I. Frequently Asked Questions

Are Internet/e-mail usage policies a mandatory subject of bargaining?

Although there is no complete list of the subjects that must be included in bargaining agreements, the National Labor Relations Act (NLRA) states that employers and union representatives must bargain in good faith about wages, hours and other work conditions.[119] In determining whether a specific policy is a mandatory subject of bargaining, the court must determine whether the policy at issue "settle[s] an aspect of the relationship between the employer and the employees."[120] Courts have held that modifications of disciplinary rules and codes of conduct should be mandatory bargaining subjects.[121] Therefore, modifications to e-mail and Internet policies that impact working conditions and could result in discipline should be considered mandatory subjects of bargaining. For instance, in *Johnston School Committee v. Rhode Island State Labor Relations Board*, the Supreme Court of Rhode Island found that a change in the employer's Internet and e-mail usage policy was a mandatory subject of bargaining because it could result in disciplinary action.[122]

To assist locals, the IAFF prepared a Model Social Media Policy that locals may use in bargaining with Fire Departments.

[119] *See* 29 U.S.C. §§ 158(a)(5), (d).
[120] *Allied Chem. & Alkali Workers, Local Union No. 1 v. Pittsburgh Plate Glass Co.*, 404 U.S. 157, 178 (1971).
[121] *See, e.g., Beverly Health & Rehab. Servs. v. NLRB*, 297 F.3d 468, 483 (6th Cir. 2002); *NLRB v. Amoco Chems. Corp.*, 529 F.2d 427, 431 (5th Cir. 1976).
[122] *Johnston Sch. Comm. v. R.I. State Labor Relations Bd.*, C.A. No. PC 03-0141, 2004 R.I. Super LEXIS 67, *26 (R.I. Apr. 5, 2004).

Online Fundraising

I. Frequently Asked Questions

Can a local use its web site to fundraise or to solicit donations online?

Yes. A local's web site can be an incredible resource for fundraising and soliciting donations from members and the community. However, there are certain steps and precautions locals must take before launching an online fundraising campaign.[123]

Most states regulate non-profit fundraising through statutes called "solicitation laws" that are "primarily concerned with the solicitation of charitable contributions from the general public," and require some type of compliance reporting by the non-profit organizations, in this case, the locals.[124] Compliance reporting under state solicitation laws is divided into two parts, registration and annual financial reporting. Registration "provides an initial base of data and information about an organization's finances and governance."[125] Annual financial reporting "keeps the states apprised about the organization's operations with an emphasis on fundraising results and practices," and generally requires an audit and the filing of certain tax forms with the state.[126] Generally speaking, "states require both registration (at least initially) and annual financial reporting."[127]

Any non-profit conducting a charitable solicitation within a given state, regardless of the method it chooses (e.g., a letter, phone call, newspaper advertisement requesting financial support from a state's residents, or e-mail), is subject to that state's laws and may be required to register before soliciting contributions.[128] However, there is little consistency with regard to the application of solicitation laws among the various states. For instance, some states require a one-time registration while others may require annual renewal of registration, submission of every common governance and financial document, or simply submission of an IRS 990 Form.[129] With approximately forty states regulating non-profits in this manner, these inconsistencies make it increasingly difficult for locals to conduct fundraising activities on a multi-state or national level.

Although most states have adopted laws that regulate charitable solicitations, it is unclear how these laws apply to online fundraising. On March 14, 2001, the National Association of State Charity Officials (NASCO) approved the Charleston Principles, which provide advisory

[123] For more information on online fundraising and charitable activities, we recommend that local affiliates consult the IAFF Local Charitable Activities Manual.
[124] National Association of Attorneys General, National Association of State Charities Officials, and Multistate Filer Project, Inc., *Standardized Registration for Nonprofit Organizations Under State Charitable Solicitation Laws*, http://www.multistatefiling.org (last accessed October 8, 2014).
[125] *Id.*
[126] *Id.*
[127] *Id.*
[128] *Id.*
[129] *Id.*

guidelines for online fundraising and explain the circumstances under which non-profits are required to register.[130] While these guidelines are not enforceable under state law, they provide a roadmap for non-profit organizations who wish to fundraise online.

As a general rule, locals must always register in their home state if they use the Internet to conduct charitable solicitations. In addition, locals that fundraise online must register in states outside of their home state if certain conditions are met. For instance, a local must register in another state if it solicits contributions through an interactive web site, i.e. a web site where the entire transaction can be completed online, and the local either: (i) specifically targets individuals physically located in that state for donations, or (ii) receives contributions from individuals in that state on a repeated and ongoing, or substantial basis through its web site.[131] Furthermore, even where a local's web site is not interactive, the local still must register if: 1) the local meets either element (i) or (ii) outlined above, and 2) the local either: (i) invites further offline activity to complete a contribution, i.e., provides an address to which a donation can be mailed or directs individuals to a phone number where they can make donations, or (ii) contacts individuals in that state by sending e-mails or other communications promoting the web site.[132]

However, locals do not have to register solely because they maintain a web site, even if they receive out-of-state and unsolicited donations. Locals that maintain web sites that provide general information to their members and the public are not subject to state solicitation laws as long as they do not use the site for fundraising. However, locals must keep in mind that, prior to contacting an out-of-state donor to solicit additional donations (for instance, if the local maintains a database of donors for future solicitation purposes and later wishes to contact those donors), the local must be registered in those states in which the donors live.

It is also important to point out that, regardless of whether or not a local is registered in a particular state, a state can enforce its laws against a local if the local's online solicitations mislead or defraud individuals physically located within that particular state. In other words, if a local in one state defrauds or misleads an individual in another state, the local will be subject to the laws of the state in which the individual was defrauded or misled.

Finally, because the registration and annual financial reporting requirements are complex in nature and vary widely from state to state, and because the failure to comply with these requirements could result in large fines and penalties, local affiliates who wish to fundraise, both generally and online, should consult their local attorney to ensure that they are in compliance with state and local laws.

---

[130] National Association of State Charity Officials, *The Charleston Principles: Guidelines on Charitable Solicitations Using the Internet*, http://www.nasconet.org/wp-content/uploads/2011/05/Charleston-Principles-Final.pdf (last accessed October 8, 2014).

[131] The Charleston Principles define "repeated and ongoing" and "substantial" as "contributions within the entity's fiscal year, or relevant portion of fiscal year, that are of sufficient volume to establish the regular or significant (as opposed to rare, isolated, or insubstantial) nature of those contributions." *Id.*

[132] *Id.*