



## Surreptitious Workplace Recording — and what to do about it

Employees, contractors, visitors and spies are the threat. Smartphones, fake key fobs, and mini voice recorders disguised as USB sticks<sup>1</sup> are some of their tools.

Motives vary.



**Industrial Espionage** – The theft of trade secrets by the removal, copying or recording of confidential or valuable information.<sup>2</sup>

**HR Issues** – One-third of employees who visit the U.S. Equal Employment Opportunity Commission (EEOC) office to file discrimination complaints bring secretly made recordings.<sup>3</sup> Katrina Patrick, a lawyer who represents aggrieved employees, says that more than 50 percent of the people who come to her office bring digital evidence. Some cases are settled for six figure sums.<sup>4</sup> One case is now in its eight year.<sup>5</sup> Either way, its expensive.

**Blackmail** – Recordings force outcomes. Recently, three employees bugged their boss for a promotion, literally. They hid a recorder in his office and tried to blackmail him with the video footage.<sup>6</sup>

**Sex** – Spycams placed in areas where there is an expectation of privacy (locker-rooms, business provided restrooms, etc.). The problem is epidemic.<sup>7</sup> Inspecting these areas is now a regular part of our client's due diligence inspections.

### Tips for Management

- Assume your discussions are being recorded.
- Before proceeding, ask if they are recording.
- Be professional. If you would not say it in a courtroom, don't say it.
- **Red Flag** – When an employee tries to recreate a previous conversation with you.
- Have an independent sweep team conduct periodic due diligence debugging inspections.

### Create a Workplace Recording Policy

- Clearly define the purpose of the policy, e.g.
  - to encourage an atmosphere for honest and open workplace communications,
  - to protect trade secrets, confidential and proprietary information,
  - to protect employee privacy. (against spycams in restrooms, showers, changing rooms, etc.)
- List the types of recordings you prohibit. (audio, video, data)
- Make it clear the policy covers everything business-related; on *and* off premises.
- List who may, and under what conditions, create exemptions to the policy.
- Define specific conditions where recording is permissible, e.g.
  - as part of the manufacturing process,
  - customer service quality control,
  - when specifically relevant to Section 7 of the National Labor Relations Act.<sup>8</sup>

<sup>1</sup> [http://youtu.be/\\_9sPngNqsfA](http://youtu.be/_9sPngNqsfA)

<sup>2</sup> <http://www.investopedia.com/terms/i/industrial-espionage.asp>

<sup>3</sup> <http://www.chron.com/business/sixel/article/One-third-of-workers-with-beefs-tape-their-bosses-1684505.php>

<sup>4</sup> <http://www.businessinsider.com/smartphones-spying-devices-2011-7>

<sup>5</sup> <http://spybusters.blogspot.com/2014/01/the-annabel-melongo-eavesdropping-case.html>

<sup>6</sup> <http://spybusters.blogspot.com/2013/10/bugging-boss-for-raise-lands-three.html>

<sup>7</sup> <http://spybusters.blogspot.com/2012/12/spycam-story-664-this-month-in-spycam.html>

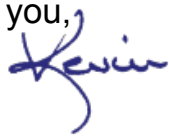
<sup>8</sup> <http://www.nlrb.gov/resources/national-labor-relations-act>

Additional free information is available at:

<http://www.counterespionage.com/download.html>

Want to know more? Just send me an email — [murray@counterespionage.com](mailto:murray@counterespionage.com)

Thank you,

A handwritten signature in blue ink that reads "Kevin". The signature is written in a cursive style with a large, sweeping initial 'K'.