UNITED STATES DISTRICT COURT

DISTRICT OF NEW MEXICO

STC.UNM,

Plaintiff,

v.

INTEL CORPORATION,

Defendant.

Civil No. 1:10-cv-01077-RB-WDS

DECLARATION OF STEVEN LUND IN SUPPORT OF INTEL'S OPPOSITION TO STC'S MOTION TO COMPEL AND IN SUPPORT OF INTEL'S MOTION TO AMEND THE INTERIM PROTECTIVE ORDER

1. My name is Steven Lund. I have personal knowledge of the facts stated below and would testify that they are true if asked to do so. I am making this declaration (1) to oppose STC's efforts to discover commercially valuable and carefully guarded trade secret information about research and development into future manufacturing technology that will not be complete or used to make commercial products until after the patent that STC is asserting against Intel has expired, and (2) to support Intel's motion for a protective order.

2. I am the Director of Corporate Security at Intel. I joined Intel in 1993 and have worked in Corporate Security since my first day on the job. I started as an investigator, charged with looking into breaches of security. Currently, I am in charge of all security systems, physical security, investigations, and risk assessment. I also sit on internal Intel management review committees that set security policy. I am familiar with Intel's security policies and procedures governing electronic information.

A. Employee Training

3. Because Intel's most important assets are its intellectual property, including its process technology data and documentation ("process information"), Intel adheres to comprehensive information security policies and procedures. Moreover, much of Intel's intellectual property is subject to export control, meaning that disclosure of that information to residents of certain countries can be a violation of federal law even if that person is in the United States at the time.

4. Intel's emphasis on information security starts even before a new employee is hired. A successful candidate at Intel must pass a pre-screening process that includes a criminal and educational background check and a check of previous employment.

5. The new hire confronts Intel's security on the very first page of the new hire packet, which advises that the employment agreement "signals your cooperation with Intel on several issues, including confidential and proprietary information."

6. This same packet includes Intel's policies and procedures for information security, including computer use. The policies and procedures explain that the new hire is required to safeguard the security of Intel's business information. The new hire packet also requires the employee's signature to a confidentiality clause that obligates the employee to maintain Intel's information in confidence "at all times."

7. Within 90 days of hire, a new employee must attend a training session covering Intel's policies and procedures regarding information security. Every two years, Intel employees are required to take a refresher course on Intel's information security policies and procedures.

Employees whose jobs deal with highly confidential information must take additional courses on information security. In total, Intel offers over a dozen classes on our security policy.

8. Between these refresher courses, Intel employees are reminded constantly of the importance of information security by postings on Intel's intranet, signs throughout Intel buildings, prompts for passwords, restricted access to parts of buildings, and security audits.

9. This focus on information security continues throughout an employee's tenure at Intel. On an employee's last day of work, those who held a grade level of 10 (senior managers) or above undergo an exit interview with an Intel in-house lawyer. Part of this exit interview reminds the departing employee of his or her obligation of confidentiality to Intel that remains even after his or her departure. At the discretion of a supervisor or someone from Intel Legal, any departing employee may be asked to sit for such an interview.

10. Intel emphasizes to employees that violations of the information security policies can be cause for termination, and even the basis of legal action against them.

B. Physical Security of Facilities

11. Every Intel facility has a secure lobby or access point, such that employees and guests must pass through security before entering the main portion of the building. Non-employees may not proceed past the lobby of any Intel facility unless they are an approved contingent worker (e.g., a contractor) with a "green badge" or are escorted by an Intel employee. (Intel employees wear "blue badges.") Even contingent workers who are approved to have a "green badge" are prohibited from certain areas without an Intel employee escort.

12. Green badges are issued on a temporary basis to non-employee contingent workers who have a business need to enter Intel facilities regularly, such as janitorial service

workers, auditors, or other vendors. Before anyone is issued a green badge, he or she must go through a background check and security screening that meets the scope and standards of Intel, and must agree, in writing, to be bound by Intel's information security policies.

13. Even a guest accompanied by an authorized badge holder must sign in, present identification, and have a business need to enter the building. Once inside, he or she must be in the presence of his or her sponsoring badge holder at all times, and signs posted throughout Intel's facilities encourage employees to challenge anyone who is not displaying a badge.

14. Many parts of Intel buildings are off limits even to those with a green badge. Indeed, some parts of Intel's facilities (such as rooms containing certain data storage devices, certain confidential documents, labs, and fabrication facilities) are forbidden even to most of Intel's own employees (and are locked by secondary security measures such as code, key, or additional card access) and cannot be entered unless the employee has a business need to enter and the approval of the area owner. At least once every quarter, the owner of any restricted area must audit the log of those with access rights to his or her area.

15. The database of blue and green badge holders is updated daily so no person with an expired badge can access an Intel facility (e.g., if a contingent worker's job is over or an employee is terminated from Intel's employ).

16. The badges contain a unique worldwide ID that allows RF (radio frequency) receivers within Intel facilities to track who has passed through certain doorways, including, the main door and doors leading to restricted access areas.

17. As another layer of security, all staffed lobbies and command centers have the capacity to call-up a picture of every Intel employee or green-badge contingent worker worldwide. This prevents a person from misusing someone else's badge.

C. Limitations on the Dissemination of Information Within Intel

18. Intel confidential information may be disseminated only on a need-to-know basis. That is, the information may be shared only with those who have a business justification for needing to know that information.

19. In addition, all information classified as secret (i.e., restricted secret or top secret) must be registered to a specific person. This means that every document containing Intel restricted secret or top secret information is checked out to a specific employee. That employee is personally responsible for any documents registered in his or her name.

20. Hard copies of any document containing confidential information must be stored in a locked drawer, cabinet, or desk at the end of every day. Hard copies of any document containing restricted secret or top secret information must be stored in a special Intel-approved locking cabinet. During the day, hard copies of any document that contains confidential information may not be left on a printer, fax, copy machine, or other common space.

21. When any document containing confidential information is transported in hard copy, either within Intel or outside, it must be either in the continuous physical possession of the person responsible for it or be placed in a designated container bearing a warning about the content's confidentiality.

22. Confidential information is protected even when disposed of. Hard copies of documents that contain any confidential information must be placed in locked waste receptacles

when disposed. The contents of these receptacles are periodically shredded, and this shredding is supervised in person by a member of Intel's security staff.

23. Intel's protection of electronic versions of confidential information is even more elaborate. The security measures described below apply to Intel confidential information, generally. Even greater protections are in place to safeguard electronic process information.

24. As an initial matter, a new employee is not issued a computer until he or she receives training in Intel's electronic security measures.

25. Each individual must have a user-specific password to access his or her computer. Some additional log-in credentials are required for access to certain Intel networks, shared drives, and applications. These passwords must be changed at least every 90 days, may not be the name or any personal number of the user, and may not be stored (physically or electronically) except in a supervisor's office. Strong passwords (in terms of numbers and types of characters) are typically required.

26. To further protect security, many Intel networks and databases are segregated so that employees in a certain division or unit have no access to information from other divisions or units. In addition, some divisions or units restrict sensitive information on their own databases even from some (or most) employees of that division or unit. For example, two groups of designers working on different aspects of the same process technology may not have access to each other's databases unless there is a business need for them to have that access.

27. This segregation is often enforced with second-level passwords and through a list of approved user IDs (which correspond to the unique ID of every Intel employee). If an employee's ID is not on the approved list, he or she cannot access that database. The list of

approved user IDs is maintained by the manager of the database or network, who grants approval to use his or her database or network only to those with a business need for access.

28. Intel also protects confidential information in electronic form through an array of security software, including encryption technology. Remote access to Intel's networks (for example, by Intel employees traveling on business) requires a VPN connection to ensure authentication of the user and encryption of the data transmitted.

29. All wireless and remote traffic on Intel's network is encrypted with 128-bit technology. In addition, an employee may add a layer of encryption at the application level (e.g., by enabling encryption for a meeting conducted over the Internet) when transmitting sensitive information.

30. Intel also protects the security of electronic information by guarding the integrity of its electronic network. Intel bans the connection of any personal equipment to its networks without the proper security technology enabled. Intel also prohibits employees from conducting any Intel business on email accounts other than their Intel email account (which ensures that transmission is always through a secure environment).

31. Even inaction is policed at Intel. If an employee conducts no activity on the network, or even within certain databases on the network, for more than 60 days, access is terminated automatically absent special circumstances. The employee may restore access only by calling the appropriate security officer and answering a series of questions to confirm their identity.

D. Limits on Sharing Confidential Information with Others

32. Intel permits the sharing of confidential information only under strict guidelines. When business necessity calls for the sharing of confidential information, these guidelines require that information be shared under standardized non-disclosure agreements whenever possible. Intel employees have access to a database of existing non-disclosure agreements with third parties and a list of contacts (including an in-house lawyer) for questions about any existing or contemplated non-disclosure agreement.

33. Intel reminds its employees in their semiannual training sessions always to ask whether there is a business need to share confidential information and whether a particular confidence must be shared at that place and at that time.

E. Monitoring Compliance with Information Security Policies

34. Intel employees are instructed to report any violation of any information security policy to a manager or a security officer.

35. Intel's security organizations routinely conduct spot checks of security policies by policing the physical and electronic workspace of employees to search for confidential information that is not secured properly. These spot checks include searches of offices at night to see if, for example, someone failed to secure confidential information, and continuous and random electronic trolling for confidential information out of place on the network or shared drives. Laptops must be locked to desks using cables supplied by Intel whenever an employee is not in his or her office. If Intel security finds a laptop that is not so secured, it will seize the laptop. The employee must explain why it was not secured property before it is returned.

36. Intel also employs groups who try periodically to crack security by physically invading a building or by hacking into networks or shared drives. At least annually, Intel's security organizations conduct full-blown audits of security procedures and systems.

I declare under penalty of perjury that the foregoing statements are true and correct.

Dated: 1-5-11 at Chandler, Arizona.

Steven Lund

Certificate of Service

The undersigned hereby certifies that on April 5, 2011, the foregoing document were electronically filed with the Clerk of Court using the CM/ECF system, which will automatically send notification of such filing to all counsel who have entered an appearance in this action.

ATKINSON, THAL & BAKER, P.C.

/s/ *Clifford K. Atkinson*
Clifford K. Atkinson

20336-1313/LEGAL20511283.2