UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et al., on her own behalf and on behalf of all those similarly situated,	)	
Plaintiffs,	)	
v.	)	**Civil Action No. 96-1285 (RCL)**
GALE NORTON, Secretary of the Interior, et al.,	)	
Defendants.	)	

PRELIMINARY INJUNCTION

In accordance with the memorandum opinion issued this date, and upon consideration of the Plaintiffs' Motion [2926] for a Preliminary Injunction, the opposition thereto, the reply brief, the applicable law, and the proceedings at the Evidentiary Hearing conducted by the Court on this matter, it is hereby

ORDERED that the Plaintiffs' Motion [2926] for a Preliminary Injunction is GRANTED; and it is further

ORDERED that the Court hereby enters the following Preliminary Injunction.

I. Definitions

For purposes of this Order only, the following definitions apply:

A. Information Technology System—Any computer, server, equipment, device, network, intranet, enclave, or application, or any subsystem thereof, that is used by Interior or any of its employees, agents, contractors, or other third parties in the

electronic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or other information, including without limitation computers, wireless devices (e.g. Blackberrys) and networks, voice over the Internet protocol (VOIP), ancillary equipment, devices, or similar services or protocols, including support services, software, firmware, and related resources.

B. Individual Indian Trust Assets—Lands, natural resources, monies or other assets held in trust by the Federal Government for the benefit of individual Indians or lands, natural resources, or other assets that are or were restricted against alienation for individual Indians.

C. Management—Actions that control, govern, administer, supervise, or regulate the custody, use, or disposition of Individual Indian Trust Assets.

D. Federal Record—This term is defined in 44 U.S.C. § 3301, and includes all documentary materials, regardless of physical form or characteristics, made or received under Federal law or in the transaction of public business and preserved or are appropriate for preservation as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities or because of the informational value in them.

E. Individual Indian Trust Data—Information stored in, or transmitted by or through, any Information Technology System that evidences, embodies, refers to, or relates to—directly or indirectly and generally or specifically—a Federal Record that reflects the existence of Individual Indian Trust Assets, and that at any time either:

(1) has been, or is now, used in the Management of Individual Indian Trust Assets; (2) is a title or ownership record; (3) reflects the collection, deposit, and/or disbursement or withdrawal of income or interest—imputed or actual—relating to Individual Indian Trust Assets whether or not such assets are held in a particular account or are identifiable to any particular individual Indian trust beneficiary by name, number, or other specific identifier; (4) reflects a communication with, or on behalf of, an individual Indian trust beneficiary; or (5) has been, or is now: (a) created for, or by, Interior or any bureau, office, agency, agent, or contractor thereof, or for, or by a Tribe in connection with the Management of Individual Indian Trust Assets; (b) provided to, or received by, Interior or any such bureau, office, agency, agent, or contractor thereof, or any Tribe, for use in the Management of Individual Indian Trust Assets, and (c) used or housed by Interior or any such bureau, office, agency, agent, or contractor thereof, or any Tribe, in connection with the government's Management of Individual Indian Trust Assets.

F. House—The storage by electronic means of Individual Indian Trust Data.

G. Access—The ability to gain entry into Information Technology Systems.

II. Substantive Provisions

A. Subject to the exceptions outlined in Section II(C) and II(D), it is hereby ORDERED that Interior defendants forthwith shall disconnect all Information Technology Systems that House or provide Access to Individual Indian Trust Data:

1. from the Internet;

2. from all intranet connections, including but not limited to the VPX, ESN, or any other connection to any other Interior bureau or office;

3. from all other Information Technology Systems; and

4. from any contractors, Tribes, or other third parties

B. It is further ORDERED that within twenty (20) days of this date, Interior defendants must submit declarations to the Court, in compliance with 28 U.S.C. § 1746 and LCvR 5.1(h)(2), identifying any Information Technology Systems that do not House or provide Access to Individual Indian Trust Data and explaining why such Information Technology Systems do not House or provide Access to Individual Indian Trust Data. The plaintiffs, in accordance with their discovery rights reaffirmed in Section II(F), may take discovery regarding the Interior defendants' declarations. The plaintiffs must file any response to Interior's submissions under this section within thirty (30) days of the completion of the plaintiffs' discovery. The Court will consider the parties' submissions, conduct any necessary evidentiary hearing, and order further relief as appropriate.

C. To protect against fires or other such threats to life, property, or national security, it is further ORDERED that:

1. all Information Technology Systems necessary for protection against fires or other such threats to life, property, or national security may remain connected and are exempted from disconnection under Section II(A); and

2. Interior defendants shall, within twenty (20) days of this date, provide declarations, in compliance with 28 U.S.C. § 1746 and LCvR 5.1(h)(2),

specifically identifying each and every Information Technology System that remains connected to protect against fires or other such threats to life, property, or national security. The declarants shall attest to: (a) the specific reasons such Information Technology Systems are essential to protect against fires or other such threats to life, property, or national security; (b) the specific connections that are necessary to protect against fires or other such threats to life, property, or national security; and (c) the compensating security controls and measures that defendants have implemented, or plan to implement, to protect Individual Indian Trust Data from loss, destruction, or unauthorized manipulation as a consequence of remaining connected.

3. The plaintiffs shall have twenty (20) days to file any response to Interior defendants' submission.

4. This Court will review Interior defendants' submission and declarations, and the plaintiffs' response thereto, but absent any contrary order from the Court, such systems may remain connected.

D. It is further ORDERED that Interior defendants may reconnect, for specified periods not to exceed five (5) business days per month, any Information Technology System that Houses or provides Access to Individual Indian Trust Data, for the purpose of receiving and distributing trust funds, or for the purpose of conducting other necessary financial transactions.

1. At least five (5) business days before temporarily reconnecting, Interior

defendants shall file with this Court and serve upon the plaintiffs' counsel their plan to so reconnect. Said plan shall include proposed Information Technology Systems to be reconnected, connections to be re-established, and security controls and measures to cover such reconnection.

2. This Court will review Interior defendants' plan to temporarily reconnect and any response thereto submitted by the plaintiffs, but absent a contrary order from the Court, Interior defendants may temporarily reconnect their Information Technology Systems that House or provide Access to Individual Indian Trust Data in accordance with the plan submitted under this Section.

E. It is further ORDERED that Interior defendants may, at any time, file with the Court and serve on the plaintiffs a proposal to reconnect, other than temporarily as set forth in Section II(D), any Information Technology System disconnected by this Preliminary Injunction or any prior order of this Court.

1. Interior defendants' proposal must include all of the following: (a) a uniform standard to be used to evaluate the security of all Information Technology Systems which House or provide Access to Individual Indian Trust Data within the custody or control of the United States Department of Interior, its bureaus, offices, agencies, agents, contractors, or any other third party; (b) a detailed process whereby the uniform standard will be applied to each such Information Technology System; (c) a detailed explanation of how such Information Technology System complies with

the uniform standard; (d) copies of all documentation relevant to he security of each such Information Technology System; and (e) a plan to provide monitoring and testing on an ongoing basis and quarterly reporting to this Court regarding the security of such Information Technology Systems.

2. The plaintiffs, in accordance with their discovery rights reconfirmed in Section II(F), may take discovery into Interior defendants' proposal. Any response shall be filed within thirty (30) days after the conclusion of plaintiffs' discovery.

3. The Court will conduct any necessary evidentiary hearing and decide whether a proposed Information Technology System may be reconnected and order further relief, as appropriate.

F. It is further ORDERED, in accordance with the Federal Rules of Civil Procedure, that the plaintiffs' discovery rights are reconfirmed.

1. The plaintiffs may take discovery, by deposition or otherwise, regarding the security of Information Technology Systems which may House or provide Access to Individual Indian Trust Data.

2. Consistent with this Court's April 25, 2005 Order, the scope of plaintiffs' discovery requests may include "all relevant reports, risk assessments, memoranda, and other documents, whether prepared by Interior officials or employees, officials or employees of other government agencies, or third parties," related to the security of each and every information

technology ("IT") system that houses or accesses or may house or access individual Indian trust data.

3. The parties shall endeavor to agree upon and submit to the Court, within ten (10) days of this date, a proposed protective order to govern disclosure of information and materials related to IT security. In the event that the parties are unable to agree on a proposed protective order, each party must submit a proposed protective order to the Court within ten (10) days of this date.

SO ORDERED.

Signed by Royce C. Lamberth, United States District Judge, October 20, 2005.